ギガビットネットワーク向けブロードバンドルーター

CentreCOM® AR570S

取扱説明書

CentreCOM AR570S

取 扱 説 明 書

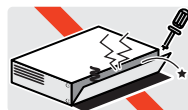
アライドテレシス株式会社

安全のために

必ずお守りください

警告 下記の注意事項を守らないと**火災・感電**により、**死亡や大けが**の原因となります。

分解や改造をしない

本製品は､取扱説明書に記載のない分解や改造はしないでください。
火災や感電、けがの原因となります。

分解禁止

雷のときはケーブル類・機器類にさわらない

感電の原因となります。

雷のときはさわらない

異物は入れない　水は禁物

火災や感電の恐れがあります。水や異物を入れないように注意してください。万一水や異物が入った場合は、電源プラグをコンセントから抜いてください。(弊社のサポートセンターまたは販売店にご連絡ください。)

異物厳禁

通気口はふさがない

内部に熱がこもり、火災の原因となります。

ふさがない

湿気やほこりの多いところ、油煙や湯気のあたる場所には置かない

内部回路のショートの原因になり、火災や感電の恐れがあります。

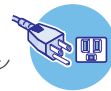
設置場所注意

表示以外の電圧では使用しない

火災や感電の原因となります。
本製品はAC100 - 240Vで動作します。
なお、本製品に付属の電源ケーブルは100V用ですのでご注意ください。

電圧注意

正しい電源ケーブル・コンセントを使用する

不適切な電源ケーブル・コンセントは火災や感電の原因となります。
接地端子付きの3ピン電源ケーブルを使用し､接地端子付きの3ピン電源コンセントに接続してください。

３ピンコンセント

コンセントや配線器具の定格を超える使い方はしない

たこ足配線などで定格を超えると発熱による火災の原因となります。

たこ足禁止

設置・移動のときは電源プラグを抜く

感電の原因となります。

プラグを抜け

電源ケーブルを傷つけない

火災や感電の原因となります。
電源ケーブルやプラグの取扱上の注意：

- 加工しない、傷つけない。
- 重いものを載せない。
- 熱器具に近づけない、加熱しない。
- 電源ケーブルをコンセントから抜くときは、必ずプラグを持って抜く。

傷つけない

ご使用にあたってのお願い

次のような場所での使用や保管はしないでください

- 直射日光のあたる場所
- 暖房器具の近くなどの高温になる場所
- 急激な温度変化のある場所（結露するような場所）
- 湿気の多い場所や、水などの液体がかかる場所（湿度80%以下の環境でご使用ください）
- 振動の激しい場所
- ほこりの多い場所や、ジュータンを敷いた場所（静電気障害の原因になります）
- 腐食性ガスの発生する場所

静電気注意

本製品は、静電気に敏感な部品を使用しています。部品が静電破壊する恐れがありますので、コネクターの接点部分、ポート、部品などに素手でふれないでください。

取り扱いはていねいに

落としたり、ぶつけたり、強いショックを与えないでください。

お手入れについて

清掃するときは電源を切った状態で

誤動作の原因になります。

機器は、乾いた柔らかい布で拭く

汚れがひどい場合は、柔らかい布に薄めた台所用洗剤（中性）をしみこませ、堅く絞ったもので拭き、乾いた柔らかい布で仕上げてください。

ぬらすな

中性洗剤使用

堅く絞る

お手入れには次のものは使わないでください

石油・みがき粉・シンナー・ベンジン・ワックス・熱湯・粉せっけん
（化学ぞうきんをご使用のときは、その注意書に従ってください。）

シンナー類不可

0 はじめに

この度は、CentreCOM AR570S をお買いあげいただき、誠にありがとうございます。

CentreCOM AR570S（以下本製品）は、ギガビットネットワーク向けブロードバンドルーターです。L2TP や IPsec による VPN で、インターネット経由の LAN 間接続が可能です。また、PIC ベイに拡張モジュールを装着することにより、ISDN 回線、デジタル専用線、フレームリレーの利用も可能です。

0.1 最新のファームウェアについて

弊社は、改良（機能拡張、不具合修正など）のために、予告なく本製品のファームウェアのバージョンアップやパッチレベルアップを行うことがあります。最新のファームウェアは、弊社 Web ページから入手してください。

参照 本書「11 バージョンアップ」（p.67）

なお、最新のファームウェアをご利用の際は、必ず弊社 Web ページに掲載のリリースノートの内容をご確認ください。

http://www.allied-telesis.co.jp/

0.2 マニュアルの構成

本製品のマニュアルは、次の 4 部で構成されています。各マニュアルをよくお読みのうえ、本製品をただしくご使用ください。また、お読みになった後も、製品保証書とともに大切に保管してください。

取扱説明書（本書）

はじめて本製品に触れるお客様が､本製品を使い始めるための情報が記載されています。また、章を読み進むごとに、段階を追って理解を深めていけるよう､ストーリーだてた構成となっています。

本書には、紙面の都合により、基本的な情報のみが記載されております。より高度な設定のための情報は、CD-ROM の「コマンドリファレンス」「設定例集」をご覧ください。

本書は、本製品のファームウェアバージョン「2.7.5.B-03」をもとに記述されていますが、「2.7.5.B-03」よりも新しいバージョンのファームウェアが搭載された製品に同梱されることがあります。本製品のご使用に当たっては、必ず弊社 Web ページに掲載のリリースノートをお読みになり､最新の情報をご確認ください。

リリースノート（弊社ホームページに掲載）

ファームウェアリリースで追加された機能、変更点、注意点や、取扱説明書とコマンドリファレンスの内容を補足する最新の情報が記載されています。リリースノートは本製品には同梱されていません。弊社Web ページに掲載されています。

http://www.allied-telesis.co.jp/

コマンドリファレンス（付属 CD-ROM）

コマンドや、コマンドが取るパラメーターの詳細、機能の解説が記載されています。本書の内容を含む、本製品の完全な情報が記載されており、関連する設定例へのリンクがあります。

付属の CD-ROM をコンピューターの CD-ROM ドライブに挿入すると、自動的に Web ブラウザーが起動し、HTML 形式のメニューが表示されます。

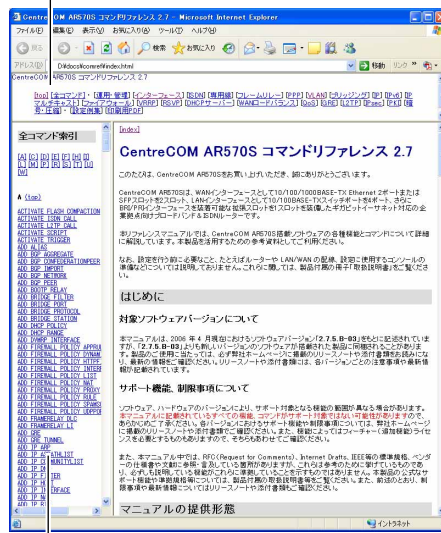
トップメニュー(機能)

サブメニュー(コマンド､機能の解説､設定例)

図 0.2.1 コマンドリファレンス

設定例集（付属CD-ROM）

具体的な構成例を図解で示し、構成に関する設定の要点を簡潔に説明したマニュアルです。構成例のリストは、番号順、回線別、機能別にソートして、簡単に設定例を探しあてられるよう工夫されています。

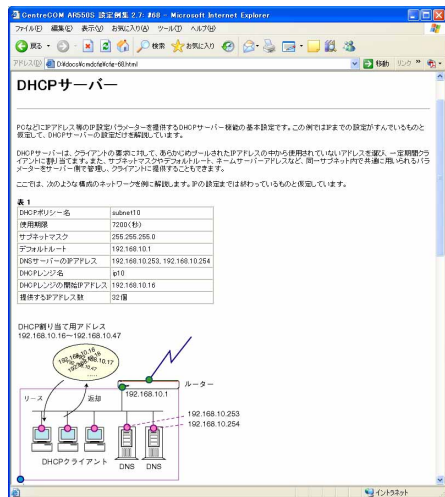



図0.2.2 設定例集

0.3 表記について

アイコン

本書で使用しているアイコンには、次のような意味があります。

アイコン	意 味	説 明
ヒント	ヒント	知っていると便利な情報、操作の手助けになる情報を示しています。
注意	注意	物的損害や使用者が傷害を負うことが想定される内容を示しています。
警告	警告	使用者が死亡または重傷を負うことが想定される内容を示しています。
参照	参照	関連する情報が書かれているところを示しています。

図0.3.1

キー入力における表記

- 「Ctrl/ △」は、Ctrl キーを押しながら、△キーを押す操作を表します。
- 「○ , △」は、○キーを押し、○キーを離してから、△キーを押す操作を表します。

例　「Ctrl/K, Ctrl/X」は、Ctrl キーを押しながら K キーを押し、Ctrl と K キーを離して、Ctrl キーを押しながら X キーを押します（Ctrl キーを押しながら K キーを押し、K キーのみを離して、X キーを押してもかまいません）。

画面表示

- コンソールターミナルに表示された内容や入力した文字を説明する場合、枠線で囲んでいます。
- 入力する文字を明示的に示す場合、**太文字**を使用します（下記の例では「HELP」）。
- 太文字以外の表示は、自動的に表示される文字です。
- コマンドを最後まで入力したら、リターンキーまたはエンターキーを 1 度押します（以後「リターンキーを押す」というように表現します）。

リターンキーは、「↵」マークで表します。下記では、「HELP」を入力し、リターンキーを押しています。

```
Manager > HELP ↵

          AR570S オンラインヘルプ - V2.7 Rev.00 2005/11/01

 This online help is written in Japanese (Shift-JIS).

 ヘルプは次のトピックを説明しています。
 入力は大文字の部分だけでかまいません（"HELP OPERATION" は "H O"と省略可）。
 （# マーク付きの機能は追加ライセンスが必要です ）

   Help Operation       運用・管理（SNMP、ログ、トリガー、スクリプトなど）
   Help INterface       インターフェース（スイッチ、ETH、BRI、PRI など）
   Help ISdn            ISDN
   Help Tdm             専用線
   Help FRamerelay      フレームリレー
   Help PPp             PPP
   Help VLan            VLAN
   Help Bridge          ブリッジング
   Help IP              IP（RIP、OSPF、IPフィルターなど）
   Help IPV6            IPv6
   Help FIrewall        ファイアウォール
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

図 0.3.2 表示画面の例

- 長いコマンドを紙面の都合で折り返す場合は、2 行目以降を字下げして表します。実際にコマンドを入力する場合は、字下げされている行の前でスペース 1 つを入力してください（下記では、「SM=...」「DM=...」「AC=...」の前にスペースが 1 つ入っています）。すべての行を入力し、最後にリターンキーを押してください。

```
ADD IP FILT=1 SO=192.168.20.4
    SM=255.255.255.255 DES=192.168.10.2
    DM=255.255.255.255 DP=23 PROT=TCP SESS=ANY
    AC=INCL ↵
```

図 0.3.3 紙面の都合でコマンドに折り返しがある例

デフォルト

デフォルトは、何も指定しなかったときに採用されるもの、パラメーターなどを省略したときに採用される数値、またはご購入時設定を意味します。

製品名

本書では、「CentreCOM AR570S」を「本製品」と略します。

固有の文字列、グローバル IP アドレスについてのお断り

本書は、説明のために以下のような架空の文字列、グローバル IP アドレスを使用します。以下のグローバル IP アドレスは、お客様の環境でご使用いただくことはできません。実際の設定では、お客様の環境におけるものに適宜読み替えていただけますようお願い申し上げます。

- PPP 接続のためのログイン名として「site_a@example.co.jp」「site_b@example.co.jp」「site_c@example.co.jp」
- PPP 接続のためのパスワードとして「passwd_a」「passwd_b」「passwd_c」
- プロバイダーから与えられたコンピューター名として「zy1234567-a」
- プロバイダー側の DHCP サーバーとして「123.45.11.5」
- プロバイダー側の DNS サーバーのアドレスとして「87.65.43.21」「87.65.43.22」
- プロバイダー側のルーターとして「123.45.11.1」
- プロバイダーから取得したグローバル IP アドレスとして「123.45.67.80 ～ 123.45.67.87」「123.45.11.22」「12.34.56.78」

目次

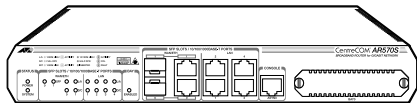
第 2 部 設定例編

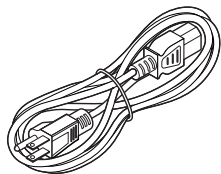
第１部　基礎編

ここでは、本製品のパッケージを開けられた時点から、ご活用いただくまでのさまざまな場面で必要となる、基本的な情報について説明します。

1.1 パッケージの確認

最初に梱包箱の中身を確認してください。

□ルーター本体 1 台

本製品の設定を行うためには、別売のコンソールケーブル（CentreCOM VT-Kit2 または VT-Kit2 plus）が必要です。

□電源ケーブル （1.8m）1 本

同梱の電源ケーブルは AC100V 用です。AC200V でご使用の場合は、設置業者にご相談ください。

同梱の電源ケーブルは本製品専用です。他の電気機器では使用できませんので、ご注意ください。

□電源ケーブル抜け防止フック 1 個

□取扱説明書 1 冊
□CD-ROM 1 枚

□製品保証書 1 枚
□シリアル番号シール 2 枚

本製品を移送する場合は、ご購入時と同じ梱包箱で再梱包されることが望まれます。再梱包のために、本製品が納められていた梱包箱、緩衝材などは捨てずに保管してください。

1.2 特長

本製品は、ギガビットネットワーク向けブロードバンドルーターです。本製品は、次のような特長を持っています。

インターネット接続と SOHO 環境の構築

WAN ポートを 2 つ、LAN 側として 4 ポートのスイッチを装備しています。他の HUB/ スイッチを用意せずに、4 台までのコンピューターを接続できます。各ポートは、10BASE-T、100BASE-TX、1000BASE-T に対応しています。

また、WAN ポートの一方を DMZ ポートとしても使用すれば、LAN 内のセキュリティを保ったまま、WAN 側に各種サーバーを公開することができます。

さまざまな回線や接続サービスをサポート

WAN ポートは、UTP ポート /SFP スロットのコンボポートとなっており、SFP モジュールを介して直接光回線を接続することが可能です。

xDSL、FTTH（10/100/1000Mbps）などのブロードバンド系サービスに対応しています。

PPPoE（PPP over Ethernet）に対応した xDSL、FTTH系のインターネット接続サービスが利用できます。PPPoE は、接続サービスが対応していれば、同時に 5 セッションまでの接続が可能です。アンナンバードによる接続に対応しておりますので、複数グローバル IP 固定割り当てサービス（アンナンバード接続）の利用も可能です。

DHCP クライアントも実装されているので、DHCP を利用したインターネット接続サービスも利用できます。

拡張スロットを装備しておりますので、PIC（Port Interface Card、別売）を装着すれば、ISDN、専用線、フレームリレーへの接続も可能です。

PPPoE セッションキープアライブ

LCP Echo や LQR パケットを使って PPP リンクの状態を監視し、自動的にPPPoE のセッションを再接続します。

IP アドレスの有効利用

NAT/EnhancedNAT により、プロバイダーから取得したグローバルアドレスを共有し、LAN 側の複数のコンピューターでインターネットを利用できます。グローバル IP 固定型のサービスを利用すれば、Web サーバーの公開も可能です。

DHCP サーバー / リレーエージェント

IP アドレス、デフォルトルート、DNS アドレスといった、LAN 環境のコンピューターの設定情報を、DHCP サーバーによって一括管理することにより、管理の労力を削減できます。また、DHCP リレーエージェントにより、他のサブネットに存在する DHCP サーバーに対して、DHCP リクエストを中継することができます。

DNS

LAN 環境のコンピューターからのDNS リクエストに対して、本製品が代理で DNS 問い合わせを行い、その結果をコンピューターに返す機能です。DHCP サーバーと併用する場合、コンピューターに通知する DNS アドレスとして、本製品の LAN 側 IP アドレスを設定しておきます。

また、DNS サーバーからの応答をメモリーに保存しておくことにより、2 回目以降の問い合わせを行わず、メモリー上の情報を参照するDNS キャッシュや、問い合わせ先のドメインごとに参照するDNS サーバーを変えることもできます。

ファイアウォールと IP フィルター

IP トラフィックフローの開始・終了を認識し、これに応じて動的なパケットフィルタリングを行うステートフル・インスペクション型のファイアウォールが搭載されています。

また、ヘッダー情報に基づき、受信 IP インターフェースにおける、パケットの破棄・通過を行う IP フィルター（トラフィックフィルター）も搭載されています。

汎用設計のIPフィルターに対して、ファイアウォールはインターネット接続を念頭に置いた設計になっており、最小限の設定で高い安全性を確保できるようになっています。ファイアウォールと IP フィルターは、運用上のニーズに応じて、使い分けたり、併用することができます。

セキュリティーを保ちながら通信コストをカット（VPN）

IPsec、L2TP、GRE により、インターネット経由の VPN が構築できます。IPsec を使用すればセキュリティーも確保できます。インターネットの利用により、ローコストのLAN 間接続が可能です。

ルーティングプロトコル

RIP V1/V2、OSPF、BGP-4 に対応しています。スタティックな経路情報も設定できます。

通信サービスの管理

ユーザーが定義したポリシーに基づき、各種トラフィックに個別のサービスレベルを割り当てるQoS 機能を備えています。このQoS 機能では、クラシファイアと呼ばれるパケットフィルターを用いてパケットをトラフィッククラスに分類し、それぞれに異なるサービスレベル（帯域、優先度など）を割り当てます。クラシファイアを用いることにより、IP アドレスや TCP/UDP ポート、DSCP（DiffServ Code Point）などに基づいた非常に細かなQoS の制御が可能です。

Priority-based ルーティングにより、受信パケットのヘッダー情報に基づき、パケットを送信するときに 8 段階の絶対優先度を設定することができます。

Policy-based ルーティングにより、受信パケットのヘッダー情報に基づき、パケットに経路選択ポリシー（サービスタイプ）を割り当て、サービスタイプに該当するパケットごとに異なる経路をとらせることできます。

RSVP（Resource reSerVation Protocol）による通信帯域の確保ができます。RSVP プロキシーエージェントにより、特定のヘッダー情報を持つトラフィックフローを検出すると、センダーやレシーバーに代わって RSVP メッセージを送信し帯域を確保します。該当のフローが無くなると自動的に帯域を開放します。

ブリッジングではプロトコル別に 5 段階の優先度を設定できます。また、LAN 側スイッチポートにおいては、VLAN タグヘッダーの IEEE 802.1p ユーザープライオリティー値に基づきパケットに送信キューを割り当てる 802.1p QoS もサポートしています。

WAN ロードバランス（AT-FL-15）

複数のWAN 回線を利用してトラフィック負荷を分散させる機能です。本機能を使用すると、特定宛先へのパケットを複数回線に振り分けることで回線負荷を分散し、帯域を有効活用できるとともに、回線ダウン時は別回線に切り替えることで WAN 接続の信頼性を高めることができます。

高い信頼性を持つIP ネットワークの構築

VRRP（Virtual Router Redundancy Protocol）をサポートしています。VRRP は、複数のルーターをグループ化して（マスターと 1 台以上のバックアップ）、あたかも 1 台のルーターであるかのように見せかけるプロトコルです。マスタールーターの故障やリンクダウンなどの障害が発生した場合、バックアップルーターがマスタールーターに昇格し、障害が発生したルーターの動作を引き継ぎます。VRRP により、システムは冗長性を持ち、高い信頼性を持つIP ネットワークを構築できます。

同一 LAN 上に複数のマスタールーターが存在する場合、複数のマスタールーターで 1 台のバックアップルーターを共有できます。

負荷分散機能により、機器や回線を有効利用することができます。

PPP 認証と IP アドレスプール

PPP による接続における認証方法として、本製品のデータベースまたは認証サーバー（RADIUS）を使用できます。接続ユーザーに対して IP アドレスを与える場合、IP アドレスプールから動的に IP アドレスを割り当てることができます。

扱いやすいファイルシステム

コンフィグレーションは、設定ファイル（テキスト）として、フラッシュメモリー（ファイルシステム）に保存されます。ファイルシステムには、複数の設定ファイルを保存しておけます。トリガーと組み合わせることにより、環境の変化に合わせて、自動的に設定を切りかえるなど、柔軟な運用が可能です。

バッチファイルによるコマンドの実行ができます。バッチファイル（.SCP）には、設定ファイル（.CFG）に直接記述できないコマンドを記述することができ、実行結果のログも出力されます。この機能は、多くのルーターを管理する場合に、非常に便利です。

TFTP、Zmodem による設定ファイルのバックアップ（アップロード）、リストア（ダウンロード）ができます。また、テキストエディターを利用して設定ファイルを編集することもできます。

システムの運用や管理

SSH（SecureShell）、Telnet による、本製品の遠隔管理ができます。

日時や曜日、特定インターフェースのリンクアップやダウンなど、様々なイベントによるトリガーを発生できます。例えば、ある時間内のみ通信を許可するといったことが可能です。

インターネットからのアタック、回線のリンク状態の変化、ログなどを、メールとして送信できます（SMTP）。

Syslog サーバーに対して、ログの出力ができます。ログは、コンソール、SSH、Telnet で確認することもできます。

NTP クライアントによる時間の同期が可能です。

SNMP をサポートしているので、インテリジェント HUB/ スイッチなどを含めた統合的なネットワーク管理が可能です。

ファームウェアインストーラーによって､ファームウェアのバージョンアップが簡単にできます。最新ファームウェア、セットアップツールは､弊社の Web ページからダウンロードできます。

機能は、本製品にロードされているファームウェアのバージョンに依存します。最新の機能は、リリースノートをご覧ください。

オプション（別売）

- SFP モジュール
  AT-MG8SX　1000BASE-SX（2 連 LC）
  AT-MG8LX　1000BASE-LX（2 連 LC）
  AT-MG8ZX　1000Mbps 光（2 連LC）

- AR シリーズ用 PIC モジュール
  CentreCOM AR020　PRIインターフェース(PRIケーブル付属)
  CentreCOM AR021 V2　BRI インターフェース

- ケーブル
  ARCBL-BRI　 BRI ケーブル
  CentreCOM VT-Kit2
  　コンソールケーブル（RJ-45/D-Sub 9 ピン（メス）変換）
  CentreCOM VT-Kit2 plus
  　コンソールケーブル（RJ-45/USB または RJ-45/D-Sub 9 ピン（メス）変換）

- 19 インチラックマウントキット
  AT-RKMT-J07

- 壁設置用ブラケット
  AT-BRKT-J22

- フィーチャーライセンス
  AT-FL-04　SMTP プロキシー
  AT-FL-05　HTTP プロキシー
  AT-FL-06　PKI
  AT-FL-08　BGP-4
  AT-FL-15　WAN ロードバランス

1.3 各部の名称と働き

図 1.3.1 前面図

図 1.3.2 LED

① STATUS LED

本製品のシステム的な状態を表示する LED です。

LED	色	状態	表示の内容
POWER	緑	点灯	本製品に電源が供給されています。
		消灯	本製品に電源が供給されていません。
SYSTEM	橙	点灯	本製品に異常が発生しています。[a]
		2 秒間隔で点滅	ファンの回転数[b] が標準の 7 割以下になっています。
		短い 6 回点滅の繰り返し	本製品の内部温度[c] がアラーム設定値を超えています。
		消灯	本製品は正常に動作しています。

a. 起動時の一時的な点灯は正常です。また、起動時の点灯から消灯への変遷は、起動の完了を示すものではありません。
b. 回転数は「SHOW SYSTEM」コマンドで確認できます。
c. 内部温度は｢SHOW SYSTEM｣コマンドで確認できます。

② WAN/ETH LED

2 つの WAN 側ポート（ETH0、ETH1）には、それぞれ SFP、L/A、D/C の 3 種類の LED が存在します。SFP LED は、SFP モジュールの状態を表示します。

LED	色	状態	表示の意味
SFP	緑	点灯	SFP モジュールを介してリンクが確立しています。
		点滅	SFP モジュールを介してパケットを送受信しています。
	橙	点灯	SFP モジュールが装着されています。
		点滅	装着された SFP モジュールに異常があります。
	ー	消灯	SFP モジュールが装着されていません。

L/A、D/C LED は、10/100/1000BASE-T ポートの状態を表示します。

LED	色	状態	表示の意味
L/A	緑	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でパケットを送受信しています。
	橙	点灯	10/100Mbps でリンクが確立しています。
		点滅	10/100Mbps でパケットを送受信しています。
	ー	消灯	リンクが確立していません。
D/C	緑	点灯	Full duplex でリンクが確立しています。
	橙	点灯	Half duplex でリンクが確立しています。
		点滅	コリジョンが発生しています。
	ー	消灯	リンクが確立していません。

③LAN LED

LAN側の各10/100/1000BASE-Tポートの状態を表示するLEDです。表示の意味は、WAN側ポートのL/A、D/C LEDと同じです。

④BAY LED

PIC ベイに装着された PIC の状態を表示する LED です。

LED	色	状態	表示の内容
ENABLED	緑	点灯	BAY0 に PIC（Port Interface Card）が装着されており、本製品によって PIC が認識されています。
		消灯	BAY0 に PIC が装着されていません。または、本製品によって PIC が認識されていません。

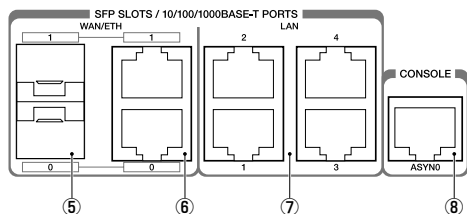



図 1.3.3 ポート

⑤WAN/ETH ポート（SFP スロット）

オプション（別売）の SFP モジュールを装着するスロットです。2 つの SFP スロットがあり、WAN 側のポートとして動作します（ETH0、ETH1）。SFP スロットは同一番号の UTP ポートとのコンボ（共有）ポートとなっています。SFP スロットに SFP モジュールが装着されているときは、同一の番号の UTP ポートは使用できません（リンクしません）。

ご購入時には、ダストカバーが取り付けられています。ダストカバーは、SFP モジュールを装着するとき以外、はずさないようにしてください。

⑥WAN/ETH ポート（UTP ポート）

WAN 側の UTP ポートです。2 つのポートがあり、1000BASE-T、100BASE-TX、10BASE-T に対応しています（ETH0、ETH1）。通信モードは、デフォルトでオートネゴシエーションが設定されています。常に MDI/MDI-X 自動切替機能が有効で、接続先のポートの種類（MDI/MDI-X）に関わらず、ストレートまたはクロスのどちらのケーブルタイプでも使用することができます。同一の番号の SFP スロットに SFP モジュールが装着されているときは、UTP ポートは使用できません（リンクしません）。

⑦LAN ポート

LAN 側の UTP ポートです。4 つのポートがあり、1000BASE-T、100BASE-TX、10BASE-T に対応しています。各ポート間の通信はスイッチングにより行われます。通信モードは、デフォルトでオートネゴシエーションが設定されています。
常に MDI/MDI-X 自動切替機能が有効で、接続先のポートの種類（MDI/MDI-X）に関わらず、ストレートまたはクロスのどちらのケーブルタイプでも使用することができます。

⑧CONSOLE ポート

本製品を設定するためのコンソールターミナルを接続する RJ-45 コネクターです。コンソールケーブルは、オプション（別売）の「CentreCOM VT-Kit2 plus」または「CentreCOM VT-Kit2」を使用してください。

⑨ BAYO

PIC（Port Interface Card）を装着するためのベイ（スロット）です。使用しない場合は、ブランクパネルを取り付けておきます。

本書「A.6 PIC（Port Interface Card）」（p.138）

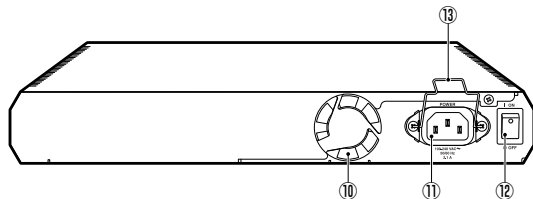



図 1.3.4 背面図

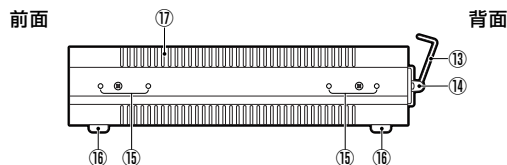



図 1.3.5 側面図

⑩ファン

内部の熱を排出するためのファンです。この穴を塞がないように設置してください。

ファンや通気口をふさいだり、周囲に物を置いたりしないでください。

⑪電源コネクター

電源ケーブルを接続するためのコネクターです。本製品に付属の電源ケーブルは AC100V 用です。AC200V でご使用の場合は、設置業者にご相談ください。

⑫電源スイッチ

本製品に供給される電源をオン、オフするためのスイッチです。

⑬電源ケーブル抜け防止フック

電源ケーブルの抜け落ちを防止する金具です（ご購入時は、フックは取り外された状態で、同梱されています）。

⑭フック取り付けプレート

電源ケーブル抜け防止フックを取り付けるプレートです。

⑮ブラケット用ネジ穴

19 インチ・ラックマウントキット（別売）を取り付けるためのネジ穴です。ラックマウントキットは、前面側または背面側に取り付けることができます。

⑯ゴム足

据え置き設置の際、本製品を固定するゴム足です。ゴム足は、本製品への衝撃を吸収したり、本製品の滑りや設置面の傷つきを防止します。

⑰通気口

換気により、本体内部の熱を逃がすための通気口です。

本製品の設置時の注意点、ラックへの取り付け、電源ケーブル抜け防止フックの取り付け、FTTH、xDSL、CATV などのブロードバンド系サービスを利用する場合の配線について説明します。ISDN 回線への接続については、付録をご覧ください。

「A.6 PIC（Port Interface Card）」（p.138）

2.1 オプションを利用した設置

本製品は卓上に設置するだけでなく、下記のオプション（別売）を利用した設置が可能です。

- ラックマウントキット AT-RKMT-J07 による 19 インチラックへの設置
- 壁設置ブラケット AT-BRKT-J22 による壁面への設置
  AT-BRKT-J22 の使用方法は、AT-BRKT-J22 の取扱説明書をご覧ください。また、設置可能な方向については、弊社 Web ページでご確認ください。

```
http://www.allied-telesis.co.jp/
```

壁設置ブラケットをご使用の際、本製品は必ず弊社 Web ページに掲載の方向で設置してください。それ以外の方向に設置すると、正常な放熱ができなくなり、火災、故障の原因となります。

ラックマウントキットや壁設置ブラケットを使用して、本製品を 19 インチラックや壁面に設置する際は、適切なネジで確実に固定してください。
不適切なネジの使用や、固定が不十分な場合、落下などにより重大な事故が発生する恐れがあります。

壁設置ブラケットに取り付け用ネジは同梱されていません。別途ご用意ください。

設置における注意

本製品の設置や保守を始める前に、必ず「安全のために」（p.4）をよくお読みください。また、次の点に注意して設置してください。

- 接続されているケーブル類に無理な力が加わるような配置や敷設はさけてください。
- テレビ、ラジオ、無線機などのそばに設置しないでください。
- 傾いた場所や、不安定な場所に設置しないでください。
- 本製品の上にものを置かないでください。
- 直射日光のあたる場所、多湿な場所、ほこりの多い場所に設置しないでください。
- 19 インチラックに設置する場合は、正しいラックマウントキットを使用してください。

2.2 19インチラックへの設置

1 ブラケットは、本製品の前面側または背面側に取り付けることができます。ブラケットの取り付け側を決めてください。

2 ラックマウントキットに付属のネジを使用し、図2.2.1 のようにブラケットと取っ手を本製品の両側面に取り付けてください。詳しくは、ラックマウントキットに付属のマニュアルをご覧ください。

3 ラックに取り付けてください（図 2.2.2）。ラックへの取り付けネジはラックマウントキットに付属しておりません。お客様でご用意ください。

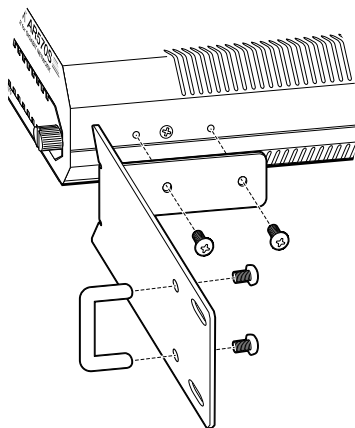



図 2.2.1 ブラケットの取り付け

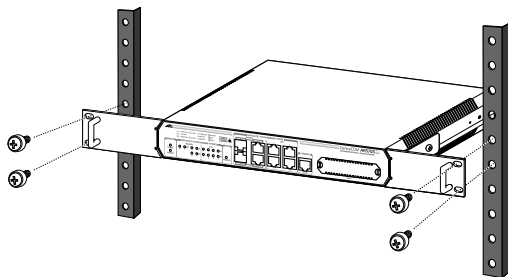



図 2.2.2 ラックへの取り付け

2.3 基本的なネットワーク構成

FTTH、xDSL、CATV などのブロードバンド系サービスを利用する場合の基本的な接続例を示します。

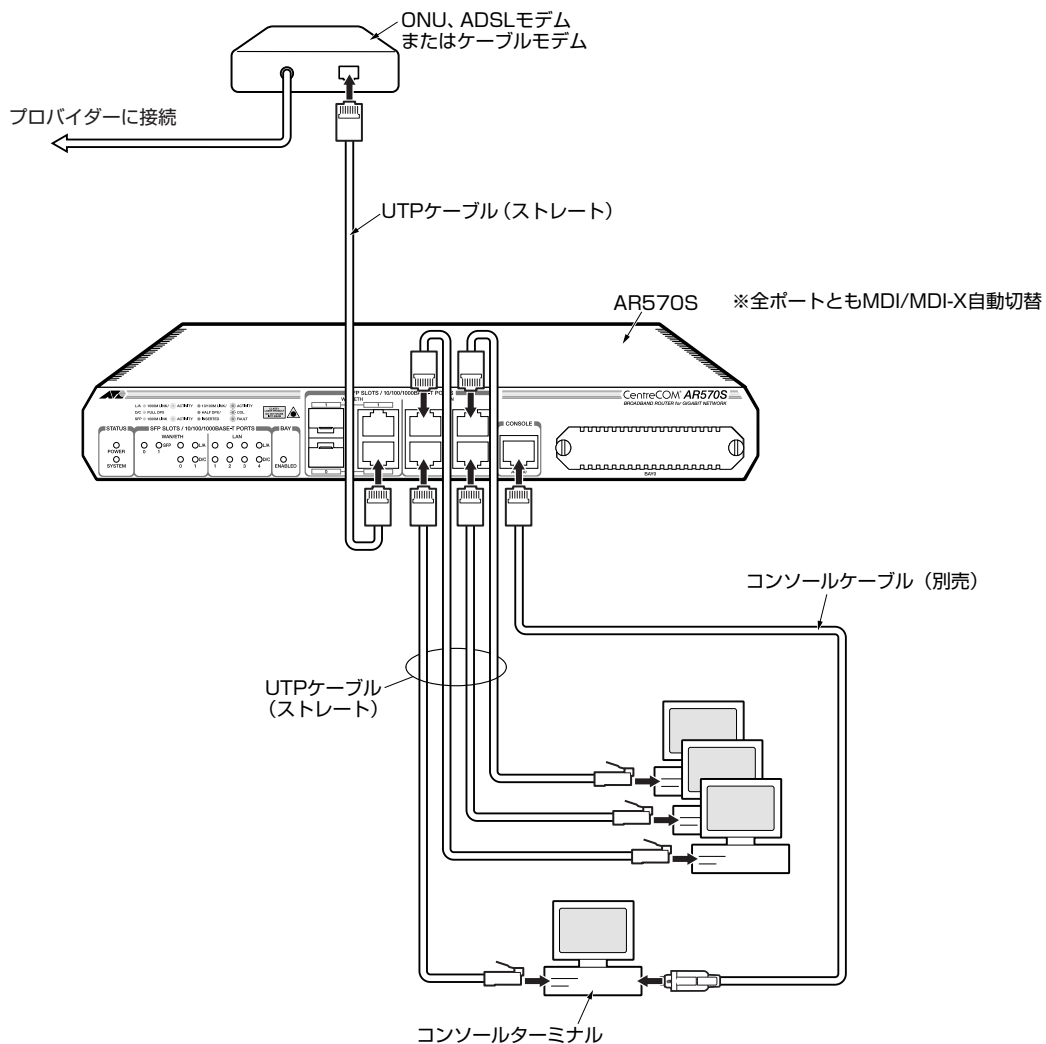



図2.3.1 ブロードバンド系サービスを利用する場合の接続例

2.4 配線

稲妻が発生しているときは、本製品の設置や、ケーブルの配線などの作業を行わないでください。落雷により感電する恐れがあります。

準備

- 19インチラックに取り付ける場合、あらかじめ「2.2 19インチラックへの設置」(p.21) に従って、設置を完了しておきます。
- 以下の手順は、回線からONU、ADSLモデムまたはケーブルモデムまでの工事(配線)が完了しているものとします。
- 10BASE-Tの場合はカテゴリー3以上、100BASE-TXの場合はカテゴリー5以上、1000BASE-Tの場合はエンハンスド・カテゴリー5のUTPケーブル(ストレートタイプ)を必要な本数だけご用意ください。各UTPケーブルの長さは、100m以内にしてください。

本製品の全ポートはMDI/MDI-X自動切替機能を持つので、ストレートまたはクロスのどちらのタイプのUTPケーブルを使用してもリンクが確立しますが、本書ではストレートタイプを使用します。

- 本製品に接続するコンピューターがTCP/IPプロトコルを使用できるように設定しておきます。

本書「A.1 コンピューターの設定」(p.131)

ONU、ADSL/ケーブルモデムの接続

1. UTPケーブルのプラグをWAN/ETH0ポートに挿入して、カチッと音がするまで差し込んでください(図2.3.1、p.22)。
2. UTPケーブルのもう一端のプラグを、ONU、ADSLモデムまたはケーブルモデムに接続してください。

コンピューターの接続

1. UTPケーブルのプラグをLANポートに挿入して、カチッと音がするまで差し込んでください(図2.3.1、p.22)。
2. UTPケーブルのもう一端のプラグを、コンピューターのネットワークポートに接続してください。
3. 手順1、手順2を繰り返し、すべてのコンピューターを本製品に接続してください。

コンソールターミナルの接続

コンソールポートを使用して、本製品の設定*1を行う場合は、コンソールターミナル(コンピューター)を接続します。

1. コンソールケーブル(別売)のRJ-45プラグを、本製品のCONSOLEポートに接続してください(図2.3.1、p.22)。
2. コンソールケーブルの D-Sub コネクターをコンピューターのCOMポートに接続し、ケーブルのネジを止めてください。COMポートは、機種により、「SERIAL」「I〇I〇I」などと表示されています。

*1 Telnetによる設定も可能です。

電源ケーブルの接続

1 付属の電源ケーブル抜け防止フックを、下図のようにフック取り付けプレートに取り付けてください。

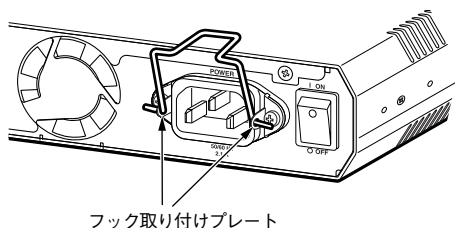



図2.4.1 電源ケーブル抜け防止フックの取り付け

2 付属の電源ケーブルを本製品背面の電源コネクターに接続してください。

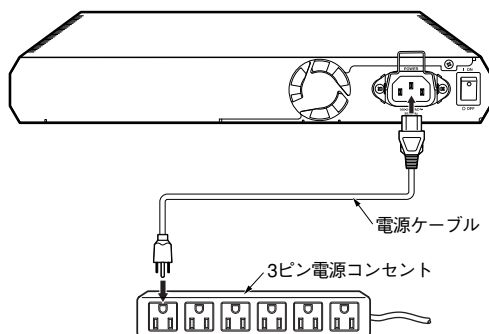



図2.4.2 電源ケーブルの接続

3 電源ケーブルのプラグを電源コンセントに接続してください。電源プラグは 3 ピンになっています。接地付きの 3 ピンコンセントに接続してください。

4 電源ケーブル抜け防止フックで、電源ケーブルが抜け落ちないようにロックしてください。

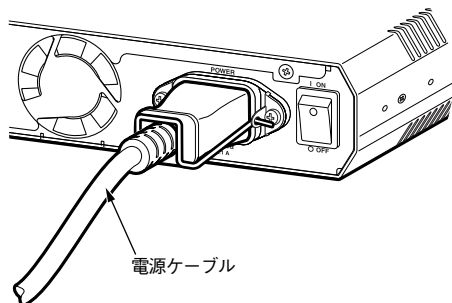



図2.4.3 電源ケーブルのロック

2.5 スイッチのカスケード接続

本製品には、4 台までのコンピューターを接続できますが、更に多くのコンピューターを接続したい場合は、スイッチや HUB をカスケード接続してください。

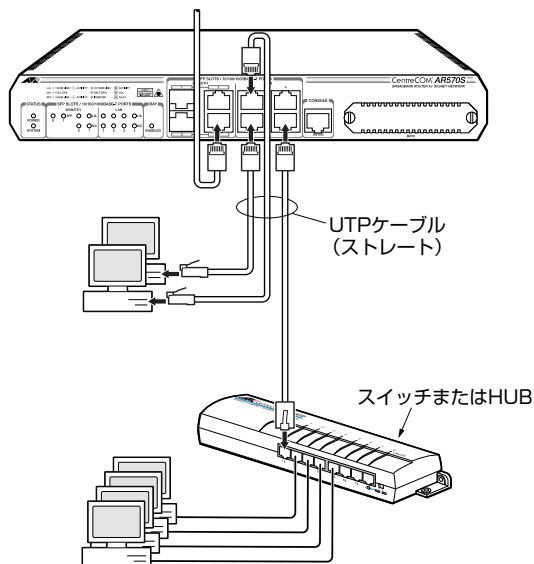



図2.5.1 スイッチの接続

1 UTP ケーブルのプラグを LAN ポートに挿入して、カチッと音がするまで差し込んでください。どのLAN ポートでもかまいません。

2 UTP ケーブルのもう一端のプラグを、スイッチまたは HUB に接続してください。

2.6 SFP モジュールの取り付け

注意

弊社販売品の SFP モジュールをご使用ください。弊社販売品以外の SFP モジュールをご使用になる場合の動作保証はしておりませんので、ご了承の程お願い申し上げます。

ヒント

SFP モジュールはホットスワップ対応のため、取り付け・取りはずしの際に、本製品の電源をオフにする必要はありません。

ヒント

SFP モジュールには、スロットへの固定・取りはずし用にハンドルが付いているタイプと、ボタンが付いているタイプがあります。形状は異なりますが、機能的には同じものです。

ヒント

光ファイバーケーブルの仕様、最大伝送距離などについては、ご使用になる SFP モジュールのマニュアルをご覧ください。

取り付け

1 SFP スロットのダストカバーをはずしてください。

2 SFP モジュールの両脇をもってスロットに差し込み、カチッとはまるまで押し込んでください。ハンドルが付いているタイプは、ハンドルを上げた状態で差し込んでください。
本製品の電源がオンになっていれば、差し込むと同時に SFP LED が橙色に点灯します。

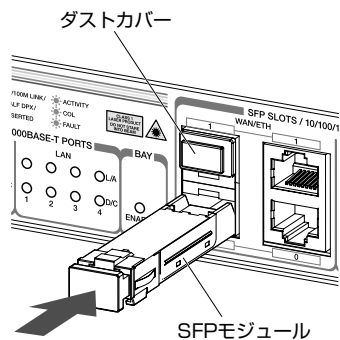



図2.6.1 SFP モジュールの挿入

注意

SFP スロット 0 に装着する場合、SFP モジュールの底面を上側にして挿入してください。
SFP スロット 1 に装着する場合、SFP モジュールの上面を上側にして挿入してください。

注意

UTP ポートがリンクアップしているときに、同一番号の SFP スロットに SFP モジュールを装着すると、UTP ポートが無効となり、リンクがダウンします。

3 SFP モジュールのダストカバーをはずしてください。

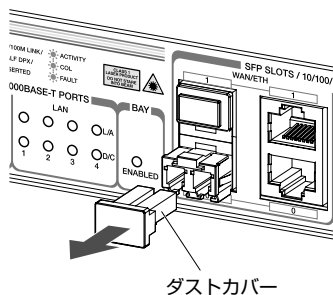



図 2.6.2

4 光ファイバーケーブルを接続してください（本製品の TX を接続先機の RX に、本製品の RX を接続先機器の TX に接続してください）。接続先機器とのリンクが確立すると、SFP LED は緑色に点灯します。

取りはずし

1 光ファイバーケーブルをはずしてください。

2 ボタンが付いているタイプは、下図のようにボタンを押し、スロットへの固定を解除します。
ハンドルが付いているタイプは、ハンドルを下げてスロットへの固定を解除します。
次に、SFP モジュールの両脇をもってスロットから引き抜いてください。

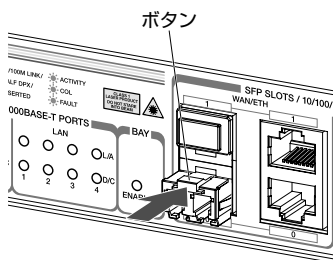



図 2.6.3

注意

SFP モジュールに光ファイバーケーブルを接続していないときは、必ずダストカバーを装着してください。

また､本製品の SFP スロットを使用していないときは､SFP
スロットにダストカバーを装着してください。

本製品の起動や停止、ログインやログアウト、本製品に施した設定の保存など、本製品を運用管理するための基本的な操作について説明します。はじめて本製品をご使用になるお客様は、この章の各節を順にお読みになることにより、本製品の運用上の特徴的な部分を理解することができます。

3.1 コンソールターミナルの設定

本製品に対する設定や管理は、背面の CONSOLE ポートに接続したコンソールターミナル、または Telnet[*1] を使用して行います。コンソールターミナルとして、下記を使用できます。

コンソールポートに接続するコンソールターミナルとして下記のものが使用できます。

- Windows 95/98/Me/2000/XP、Windows NT に付属のハイパーターミナル
- Windows 95/98/Me/2000/XP、Windows NT で動作する VT100 をサポートした通信ソフトウェア
- 非同期のRS-232 インタフェースを持つ VT100 端末装置

通信ソフトウェアに設定するパラメーターは、下記の通りです。エミュレーション、「BackSpace」キーのコードは「EDIT」コマンドのための設定です。文字セットは、「HELP」コマンド（日本語オンラインヘルプ）のための設定です。

表3.1.1 コンソールターミナルの設定

項目	値
インターフェース速度	9,600bps
データビット	8
パリティ	なし
ストップビット	1
フロー制御	ハードウェア（RTS/CTS）
エミュレーション	VT100
BackSpace キーのコード	Delete
エンコード	SJIS

コンソールターミナルとして、ハイパーターミナルを使用するための設定手順は下記をご覧ください。

 本書「A.3 ハイパーターミナルの設定」（p.134）

*1 Telnet を使って設定を行う場合、あらかじめコンソールターミナルで本製品に IP アドレスを割り当てておかなければなりません。Telnet は、本書「7 Telnet を使う」（p.57）で説明しています。

3.2 起動

1 コンピューターの電源をオンにし、ハイパーターミナル（通信ソフトウェア）を起動してください。

2 本製品の電源スイッチをオンにしてください。

3 自己診断テストが実行され、ファームウェアがロードされます。また、起動スクリプトが指定されていれば実行します。起動スクリプトが指定されていない場合は、「boot.cfg」を実行します。

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 131072k bytes found.
INFO: BBR tests beginning.
PASS: BBR test, 512k bytes found.
INFO: Self tests complete.
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download successful.

INFO: Initialising Flash File System.


INFO: IGMP packet trapping is active for IGMP snooping,
    L3FILT is activated
INFO: Router startup complete

 login:
```

図 3.2.1 ご購入時における起動メッセージ

4 login: と表示されたら、次の「3.3 ログイン（ご購入時）」にお進みください。

トラブルシューティング

うまくいかない場合は、下記をご確認ください。

「login:」と表示されない

- リターンキーを数回押してみる。
- 本製品の電源ケーブルが正しく接続されているか確認する。
- コンソールケーブルが正しく接続されているか確認する。

文字化けする

- ハイパーターミナル（通信ソフトウェア）の通信速度が9,600bpsに設定されているか確認する。
- 別のフォントを選択してみる。

それでもうまくいかないときは、一旦本製品の電源スイッチをオフにし、しばらく待ってから、電源スイッチをオンにしてみます。まだうまくいかない場合には、ハイパーターミナルを一旦終了し、再起動してみます。また、Windows を再起動してみます。

3.3 ログイン（ご購入時）

設定や管理を行うためには、本製品にログインしなければなりません。ご購入時の状態では、Manager（管理者）レベルのユーザー「manager」のみが登録されています。初期パスワードは「friend」です。初期導入時の設定作業をはじめ、ほとんどの管理、設定作業は、ユーザー「manager」で行います。

表3.3.1 ご購入時のユーザー名とパスワード

ユーザー名	manager
パスワード	friend

1 loginプロンプトが表示されたら、下記のように入力します。

```
login: manager ↵
```

2 Password プロンプトが表示されたら、下記のように入力します。実際の画面では入力したパスワードは表示されません。

```
Password: friend ↵  （表示されません）
```

3 コマンドプロンプト「Manager >」が表示されます。本製品に対する設定や管理は､このプロンプトに対してコマンドの文字列を入力することにより行います。

```
Manager >
```

本書「4.1 コマンドプロセッサー」（p.35）

3.4 パスワードの変更

1 下記のように入力します。

```
Manager > SET PASSWORD ↵
```

2 現在のパスワードを入力します。ご購入時では初期パスワード「friend」なので、下記のように入力します。ここでは説明のためパスワードを記載しますが､実際の画面では入力したパスワードは表示されません。

```
Old password: friend ↵  （表示されません）
```

3 変更後に指定する新しいパスワードを入力します（6文字以上）。ここでは新パスワードを「rivADD」と仮定します。実際の画面では入力したパスワードは表示されません。

```
New password: rivADD ↵  （表示されません）
```

4 確認のために、再度新しいパスワードを入力します。ここでは説明のためパスワードを記載しますが､実際の画面では入力したパスワードは表示されません。Confirmを入力後、コマンドプロンプトが現れない場合、再度リターンキーを押してください。

```
Confirm: rivADD ↵  （表示されません）

Manager >
```

手順3と4で入力した「新しいパスワード」が同じものであれば、本製品はパスワードの変更を受け入れます。
異なっている場合、次のメッセージが表示されますので、再度「SET PASSWORD」コマンドを実行してください。

```
Error (3045287): SET PASSWORD, confirm password incorrect.

Manager >
```

パスワードの変更が成功した場合、ユーザー「manager」の次からのパスワードは下記のようになります。

表3.4.1 次回のパスワード（本ページの例）

ユーザー名	manager
パスワード	rivADD

ユーザー「manager」のパスワードは、必ず変更してください。初期パスワードのままで運用した場合、重大なセキュリティーホールとなります。

ユーザー「manager」の変更したパスワードを忘れないでください。パスワードを忘れると、本製品にログインできなくなりますので、充分にご注意ください。

5 次の「3.7 設定の保存」（p.30）を実行してください。

ユーザー名、パスワードに使用可能な文字、ユーザーレベルなどの詳しい説明は、下記をご覧ください。

本書「5 ユーザー管理とセキュリティー」（p.49）

3.5 システム名の変更

システム名（MIB Ⅱオブジェクト sysName）を設定すると、プロンプトにシステム名が表示されるようになります。複数のシステムを管理しているときは、各システムに異なる名前を設定しておくと、どのシステムにログインしているのかがわかりやすくなり便利です。

1 下記のコマンドを実行します。下記では、システム名を「OSAKA」に設定しています。

```
Manager > SET SYSTEM NAME="OSAKA" ↵
```

2 プロンプトが「Manager OSAKA>」に変わります。

```
Info (1034003): Operation successful.

Manager OSAKA>
```

また、login プロンプトにもシステム名が表示されるようになります。

```
OSAKA login:
```

3 次の「3.7 設定の保存」を実行してください。

3.6 システム時間の設定

本製品に内蔵の時計（リアルタイムクロック）を現在の時間に合わせます。

1 現在の日時を入力します。例では、2005 年 3 月 26 日の 13 時 53 分に合わせています。

```
Manager > SET TIME=13:53:00 DATE=26-MAR-2005 ↵
```

2 下記のようなメッセージが表示されれば、時計合わせは完了です。

```
System time is 13:53:00 on Saturday 26-Mar-2005.
```

本製品の現在時刻は、「SHOW TIME」で確認することができます。

```
Manager > SHOW TIME ↵

System time is 13:54:18 on Saturday 26-Mar-2005.
```

「SET TIME」コマンドは、電池によってバックアップされたリアルタイムクロックに対して実行され、効果は電源スイッチのオフ後も持続します。そのため「CREATE CONFIG」コマンドで作成される設定スクリプトに反映されません。

NTP プロトコルによって、NTP サーバーと時間を同期することもできます。詳しくは、下記をご覧ください。

コマンドリファレンス「運用・管理」の「NTP」

3.7 設定の保存

入力したコマンドはただちに実行されますが、コマンドによって設定された内容はランタイムメモリー上にあるため、本製品の電源スイッチのオフや、再起動コマンドの実行で消失してしまいます。

現在の設定を、例えば先ほどのパスワードやシステム名を、次回の起動時に再現するために、設定スクリプトファイルを作成し、フラッシュメモリーに保存しておきます。

「CREATE CONFIG」コマンドは、ランタイムメモリー上に存在する現在の設定内容から、「その設定内容を作り出すために入力しなければならない一連のコマンド」（スクリプトファイル）を作成し、フラッシュメモリーに保存します。

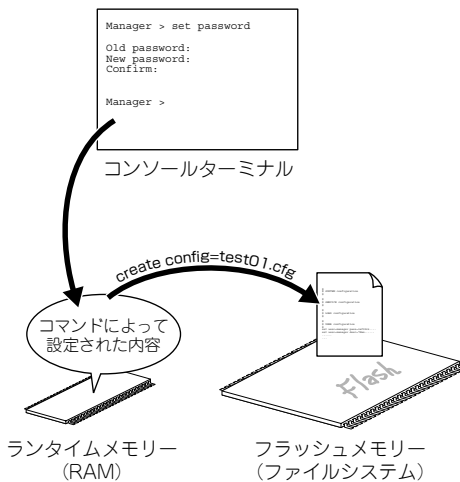



図3.7.1 スクリプトの作成と保存

1 プロンプトに対して、「CREATE CONFIG=*filename*.CFG」コマンドを入力します。この例では、設定スクリプトのファイル名を「test01.cfg」と仮定しています。

```
Manager > CREATE CONFIG=test01.cfg ↵
```

設定スクリプトのファイル名には、通常「**.cfg**」という拡張子をつけます。ファイル名部分として、16文字以内の英数半角文字とハイフン「-」が使用できます。同じ名のファイルが既に存在する場合、上書きされます。存在しない場合は、新規に作成されます。

2 ファイルが正しく作成されたことを確認してみましょう。「SHOW FILE」コマンドで、ファイル名がリスト表示されます（ファイルサイズと日付は一例です）。

```
Manager > SHOW FILE ↵

Filename           Device   Size       Created          Locks
-------------------------------------------------------------
55275b03.rez       flash  3553292  24-MAR-2006 14:37:22  0
example_isp.cfg    flash  2840     25-MAR-2006 11:29:23  0
feature.lic        flash  39       24-MAR-2006 14:55:15  0
help.hlp           flash  106718   24-MAR-2006 14:45:09  0
longname.lfn       flash  89       25-MAR-2006 19:38:58  0
prefer.ins         flash  64       24-MAR-2006 14:41:16  0
random.rnd         flash  3904     02-MAR-2006 11:09:54  0
release.lic        flash  256      15-MAR-2006 15:37:22  0
test01.cfg         flash  2840     25-MAR-2006 11:29:23  0
ud.cfg             flash  5428     18-MAR-2006 16:57:44  0
-------------------------------------------------------------
```

設定スクリプトは、テキストファイルです。「SHOW FILE」コマンドでファイル名を指定すると、内容を見ることができます。

```
Manager > SHOW FILE=test01.cfg ↵

File : test01.cfg

1:
2:#
3:# SYSTEM configuration
4:#
5:
6:#
7:# LOAD configuration
8:#
9:
10:#
11:# USER configuration
12:#
13:set user=manager pass=3af0066cad11f7a6cb5db4467bce503eff priv=manager lo=yes
14:set user=manager telnet=yes desc="Manager Account"
15:
16:#
17:# TTY configuration
18:#
--More--  (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

「スペース」バーを押すと画面がスクロールします。「Q」キーを押すと表示を終了します。

既存の起動スクリプトで動作している本製品に対して、設定を追加したときには、手順 1 の「CREATE CONFIG」で既存の起動スクリプト名を指定します。例えば、今作ったtest01.cfg に、後で IP 情報などを追加した場合には、「create config=test01.cfg」で上書き保存します。

ファイル名に使用可能な文字、ファイルシステムなどの詳しい説明は、下記をご覧ください。

本書「9 ファイルシステム」（p.61）
コマンドリファレンス「運用・管理」の「記憶装置とファイルシステム」

3.8 起動スクリプトの指定

本製品が起動するとき、作成した設定スクリプトが実行されるように設定します。起動時に実行される設定スクリプトのことを、「起動スクリプト」と呼びます。

1 「SET CONFIG=*filename*.CFG」コマンドで起動スクリプトを指定します。この例では、ファイル名を「test01.cfg」と仮定しています。

```
Manager > SET CONFIG=test01.cfg ↵
```

2 これで起動スクリプトを指定できました。現在指定されている起動スクリプトは、「SHOW CONFIG」コマンドで確認できます。

```
Manager > SHOW CONFIG ↵

Boot configuration file: flash:test01.cfg
    (exists)
Current configuration: flash:boot.cfg
    (default)
```

「Boot configuration file:」は現在指定されている起動スクリプトファイル、「Current configuration:」は起動したとき実行したスクリプトファイルです。

上記の例で「Current configuration: flash:boot.cfg」となっているのは、起動スクリプトとして「test01.cfg」は指定されているが、指定直後であり、再起動されていないことを示しています。

本書「3.2 起動」(p.27)

3.9 再起動

本製品を再起動する方法は、次の3つがあります。

- RESTART ROUTER コマンドの入力
- RESTART REBOOT コマンドの入力
- 電源スイッチのオフ / オン

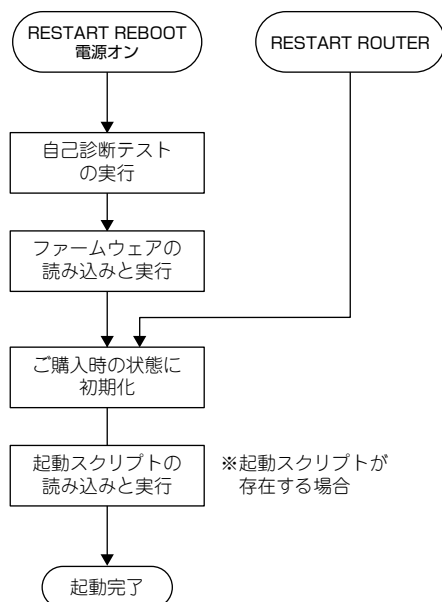



図 3.9.1 ブートシーケンス

RESTART ROUTER コマンドの入力

ソフトウェア的なリセットを行います（**ウォームスタート**）。起動スクリプトだけを読み直して設定を初期化します（起動スクリプトは「SET CONFIG」コマンドで指定します）。
起動スクリプト（*filename*.cfg）だけを変更した場合に、このコマンドを使用します。

1 プロンプトが表示された状態で、下記のように入力します。

```
Manager > RESTART ROUTER ↵
```

2 login プロンプトが表示されたら、再起動は完了です。下記では、起動メッセージにより「test01.cfg」が読み込まれたことが表示

されています。

```
INFO: Initialising Flash File System.

INFO: IGMP packet trapping is active for IGMP snooping,
    L3FILT is activated

INFO: Executing configuration script <flash:test01.cfg>
INFO: Router startup complete

 login:
```

RESTART REBOOT コマンドの入力

次の「電源のオフ / オン」と同じ動作を行うコマンドです（**コールドスタート**）。ハードウェア的にリセットされ、自己診断テストの実行、ファームウェアをロードした後、起動スクリプトを読み込み、起動スクリプトの内容による動作を開始します。本製品のファームウェアをバージョンアップした場合は、この操作を実行しなければなりません。

1 プロンプトが表示された状態で、下記のように入力します。

```
Manager > RESTART REBOOT ↵
```

2 login プロンプトが表示されたら、再起動は完了です。下記では、起動メッセージにより「test01.cfg」が読み込まれたことが表示されています。

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 131072k bytes found.
INFO: BBR tests beginning.
PASS: BBR test, 512k bytes found.
INFO: Self tests complete.
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download successful.

INFO: Initialising Flash File System.

INFO: IGMP packet trapping is active for IGMP snooping,
    L3FILT is activated
INFO: Executing configuration script <flash:test01.cfg>
INFO: Router startup complete

 login:
```

電源のオフ / オン

本製品の電源スイッチをオフにした後、オンにします。ハードウェア的にリセットされ、自己診断テストの実行、ファームウェアをロードした後、起動スクリプトを読み込み、起動スクリプトの内容による動作を開始します。本製品のファームウェアをバージョンアップした場合は、この操作を実行しなければなりません。

1 本製品の電源スイッチをオフにします。

2 しばらく待ってから、電源スイッチをオンにします。

3 login プロンプトが表示されたら、再起動は完了です。

再起動時のご注意

PPPoE によってプロバイダーと接続している場合、本製品の再起動は、PPPoE の接続が確立していない状態で行なってください。接続が確立したままで再起動してしまうと、PPPoE の接続相手の装置で矛盾が生じてしまうため、プロバイダーによっては本製品の起動後、しばらくの間再接続ができなくなることがあります。

1 「DISABLE PPP」コマンドによって、接続を正しく切断します。詳しくは、下記をご覧ください。

本書「PPPoE セッションの手動による切断」（p.128）

2 電源スイッチのオフや、「RESTART」コマンドを実行してください。

3.10 ログアウト

本製品の設定が終了したら、本製品からログアウトして通信ソフトウェアを終了します。

1 次のプロンプトが表示された状態で、下記のように入力します。

```
Manager > LOGOFF ↵
```

2 これでログアウトが完了です。ログアウトコマンドは、「LOGOFF」の代わりに「LOGOUT」や「LO」でも可能です。

通信ソフトウェア（コンソールターミナル）を終了する前に、必ずログアウトしてください。ログアウトせず通信ソフトウェアを終了すると、コンソールターミナルを使用できる誰でも Manager レベル権限を得ることができます。セキュリティーのために、必ずログアウトしてください。

3.11 停止

本製品は、下記の方法で停止します。

1 本製品にログインしている場合は、ログアウトしてください。

2 本製品の電源スイッチをオフにします。

3 これで本製品は停止しました。

3.12 ご購入時の状態に戻す

ご購入時の状態、すなわち本製品に対して設定がまったく施されていない状態に戻す手順を説明します。

1 Manager レベルでログインしてください。

```
 login: manager ↵
Password:
```

2「SET CONFIG=NONE」コマンドにより、起動時に設定スクリプトが読み込まれないようにします。詳細は、本書「3.8 起動スクリプトの指定」(p.31)をご覧ください。

```
Manager > SET CONFIG=NONE ↵
```

3「RESTART　ROUTER」コマンドを実行してください。本製品は、起動スクリプトを読み込まない状態で初期化され、初期化のためにログアウトしてしまいます。ソフトウェア的にはご購入時の状態となりますが、まだお客様が保存した設定スクリプトは削除されていません。

```
Manager > RESTART ROUTER ↵

 login:
```

「RESTART REBOOT」の実行や、電源スイッチのオフ/オンによる再起動を行なってもかまいません。

4 Manager レベルでログインしなおします（パスワードはデフォルトに戻っています）。

```
 login: manager ↵
Password: friend ↵（表示されません）
```

5 設定スクリプトのすべてを削除すると、完全にご購入時の状態となります。ファイル名をひとつひとつ指定してもかまいませんが、ワイルドカード「*」を使用するのが便利です。

```
Manager > DELETE FILE=*.cfg ↵
```

設定スクリプト(.CFG)を削除してしまうと、お客様が保存した設定は完全に失われます。

3.13 ロックアウトされてしまったとき

コンソールターミナルまたは Telnet によって本製品にログインするとき、同じユーザー名でパスワードを**連続して 5 回**間違えると、下記のメッセージが表示され、しばらくの間ログインできなくなります。

```
 login: manager ↵
Password:

Info. This device is locked out temporarily
    (login-lockout).
```

10 分(デフォルト)が経過するとロックアウトは解除され、再びログインできるようになります(電源のオフ/オンを実行すれば、即時にロックアウトは解除されます)。

本製品に登録されているユーザーアカウントに対するアクセスは、「SHOW USER」コマンドによって表示することができます。下記では、「manager」によるアクセスのうち 2 回はログインに成功、5 回失敗しています。

```
Manager > SHOW USER ↵

User Authentication Database
------------------------------------------------------------------------------
Username: manager (Manager Account)
   Status: enabled    Privilege: manager    Telnet: yes    Login: yes
   Logins: 2          Fails: 5         Sent: 0           Rcvd: 0
   Authentications: 0 Fails: 0
------------------------------------------------------------------------------


Active (logged in) Users
------------------------

User           Port/Device
    Login Time             Location
-----------------------------------------------------------------------
manager        Telnet 0
    14:12:36 26-Mar-2005     192.168.1.101
-----------------------------------------------------------------------
```

3.14 設定情報の表示

よく使用する「SHOW」コマンドを示します。画面が広いスクリーンをご使用の場合、例えば66行に設定された通信ソフトウェアをお使いの場合、「SET ASYN=asyn0 PAGE=66」を実行しておくと、最下行で「--MORE--」が表示されるようになります。

「SHOW SYSTEM」コマンドは、システムの全般的な情報を表示します。

```
Manager OSAKA> SHOW SYSTEM ↵

Router System Status                          Time 01:36:14 Date 05-Apr-2006.
Board      ID Bay  Board Name             Host Id Rev    Serial number
--------------------------------------------------------------------------------
Base      257     AR570S                        0 M2-0   D1656101A
PIC        75  0  AT-AR020-00 PIC E1/T1 PRI     0 M2-0   50087737
--------------------------------------------------------------------------------
Memory -   DRAM :131072 kB    FLASH : 32768 kB
Chip Revisions -
--------------------------------------------------------------------------------
SysDescription
CentreCOM AR570S version 2.7.5.B-03 09-Mar-2006
SysContact

SysLocation

SysName
OSAKA
SysDistName

SysUpTime
68586 ( 00:11:25 )
Boot Image      : 570-104.fbr size 771920 28-Mar-2006
Software Version: 2.7.5.B-03 09-Mar-2006
Release Version : 2.7.5.B-00 20-Oct-2005
Release built   : Mar 28 2006 at 15:15:27
Patch Installed : NONE
Territory       : japan
Country         : none
Help File       : help.hlp

Temperature     :  38 Celsius
Main Fan Speed  : 5232 RPM

Voltage Status ( Rail : Read )
  1.2V : 1.17V   2.5V : 2.55V   3.3V : 3.23V
  5.0V : 4.89V  12.0V : 11.56V

Battery voltage : 3.23V

Configuration
Boot configuration file: flash:test01.cfg (exists)
Current configuration: flash:test01.cfg

Security Mode   : Disabled

Warning (2048284): No patches found.

Manager OSAKA>
```

「SHOW CONFIG」コマンドは、現在指定されている起動スクリプトのファイル名を表示します。

本書「3.8 起動スクリプトの指定」(p.31)

「SHOW FILE」コマンドは、ファイルをリスト表示します。

「SHOW FILE=*filename*.CFG」のようにファイル名を指定すると、ファイルの内容を表示します。

本書「3.7 設定の保存」(p.30)

「SHOW CONFIG DYNAMIC」コマンドは、ランタイムメモリー(RAM)上の設定内容を表示します。設定をスクリプトファイルとして保存する前に、このコマンドで確認するのが便利です。

```
Manager OSAKA> SHOW CONFIG DYNAMIC ↵

#
# SYSTEM configuration
#
set system name="OSAKA"

#
# SERVICE configuration
#

#
# LOAD configuration
#

#
# USER configuration
#
set user=manager pass=3af5001f767b664cad1ceb3eff0c6ab5d4 priv=manager lo=yes
set user=manager desc="Manager Account" telnet=yes

#
--More--  (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

「SHOW CONFIG DYNAMIC=*module-id*」のように機能モジュール名を指定すると、その部分だけが表示されます。機能は、SYSTEM、IP、PPP、DHCP、INT、SNMP、TELNET、USERなどが指定できます。

```
Manager OSAKA> SHOW CONFIG DYNAMIC=SYSTEM ↵

#
# SYSTEM configuration
#
set system name="OSAKA"

#
# SERVICE configuration
#
```

4 設定のための基礎知識

コンソールターミナルまたは Telnet で本製品にログインすることにより、本製品に対する設定を施すことができます。本章では、設定を施すためのコマンド入力に関する基本的操作方法、コマンドの分類、ソフトウェア的な内部構造、インターフェース名について説明します。

4.1 コマンドプロセッサー

コマンドプロセッサーは、文字ベースの対話型ユーザーインターフェースです。

ユーザーが本製品にログインすると、コマンドプロセッサーはコマンドの入力を促すためにコマンドプロンプトを表示します。コマンドプロンプトは、ログインしているユーザーの権限レベルと、システム名が設定されているか否かによって、次のように変化します。

表4.1.1

権限レベル	システム名設定なし	システム名設定あり[a]
User	>	OSAKA>
Manager	Manager >	Manager OSAKA>
Security Officer	SecOff >	SecOff OSAKA>

a. システム名「OSAKA」の場合。

本書「5 ユーザー管理とセキュリティー」(p.49)
本書「3.5 システム名の変更」(p.29)

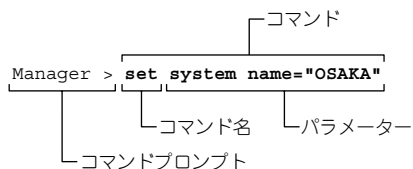



図4.1.1 コマンドの構成

コマンドプロンプトに対してコマンドを入力すると、コマンドプロセッサーは、コマンドを解析し実行します。コマンドは、コマンド名(行頭のキーワード)とパラメーター(先頭のキーワードに従属するキーワード)から構成され、スペースで区切って羅列します。

パラメーターは、上図の「SYSTEM」のように値を持たないものと、「NAME="OSAKA"」のように値(PARAMETER=*value*)を持つものがあります。

パラメーターが連続する場合、先行して入力したパラメーターによって、後続のパラメーターが限定されることがあります。

本書「次に選択可能なキーワードを表示する「?」」(p.36)

コマンドを入力し、実行に成功すると、「.... successful」というメッセージが表示されます。

```
Manager > SET SYSTEM NAME="OSAKA" ↵

Info (1034003): Operation successful.
```

図 4.1.2 成功メッセージ例

入力ミスなどにより、コマンドの実行に失敗すると、「Error」で始まるメッセージが表示されます。

```
Manager > SEG SYSTEM NAME="OSAKA" ↵

Error (335256): Unknown command "seg".
```

図 4.1.3 失敗メッセージ例

コマンド入力の注意点

コマンド入力における注意点をまとめます。

- 1行で入力できるコマンドの最大文字数は、スペースを含めて1000文字[*1]です。通常の用途では事実上無制限ですが、コマンド行が長くなり1行におさまらない場合は、ADD と SET または CREATE と SET の組み合わせを使って、コマンドを複数行に分けるか、次の省略形を使ってください。

  本書「コマンドの分割入力」(p.36)

- コマンド名やパラメーターは、省略形が使用可能です。
  例えば、「SHOW PORT」は「SH PO」、「HELP SHOW PORT」は「H SH PO」のように省略できます。

  本書「次に選択可能なキーワードを表示する「?」」(p.36)

- コマンド名やパラメーターは、大文字、小文字を区別しませんが、値として文字列が与えられている場合、値は大文字、小文字を区別することがあります(例えば、パスワード、システム名など)。

- ログインユーザーの権限によって、実行できるコマンド名が異なります。通常の管理作業は、Manager レベルで行います。セキュリティーモードでは、Security Officer レベルの権限が必要です。

  本書「5 ユーザー管理とセキュリティー」(p.49)

*1 システム名が設定されている場合(SET SYSTEM NAME)、入力可能な文字数は、システム名の文字数だけ短くなります。

- コマンドの効果は、コマンドを入力するとただちに現れます（エラーがなければ）。再起動などを行う必要はありません。
ただし、本製品を再起動すると設定内容は消失してしまうので、設定をスクリプトとして保存し、起動時に読み込まれるように設定しておかなければなりません。

本書「3.7 設定の保存」（p.30）
本書「3.8 起動スクリプトの指定」（p.31）

キー操作（ヒストリー機能）

コマンドプロンプトに対してカーソルが表示されている行、すなわちコマンドを入力しようとしている行のことをコマンドラインと言います。コマンドラインでは、次のような編集機能を使用できます。下記の表において、「Ctrl/ □」は Ctrl キーを押しながら、「/」の後のキーを押すことを意味します。

表 4.1.2 コマンドラインにおける編集キー

機能	VT 端末のキー
コマンドライン内のカーソル移動	←、→
カーソル左の 1 文字削除	Delete、Backspace
挿入モード、上書きモードの切り替え	Ctrl/O
コマンドラインの消去	Ctrl/U
入力したコマンドの履歴をさかのぼる	↑、Ctrl/B
入力したコマンドの履歴を進める	↓、Ctrl/F
入力したコマンドの履歴のすべてを表示する	Ctrl/C 「SHOW ASYN HISTORY」の入力
コマンドの履歴のすべてを消去する	「RESET ASYN HISTORY」の入力
最後に入力した *string* で始まるコマンドを表示する	*string*＋タブ（Ctrl/I）

次に選択可能なキーワードを表示する「?」

「?」は特別な意味を持つキーです。コマンドの入力途中で押すと、次に選択可能なキーワード（コマンド名、パラメーター）のリストを表示します。

コマンドプロンプトに対して、「?」キーを押してみてください。コマンドのトップレベルで使用可能なキーワード（コマンド名）が表示され、再びコマンドプロンプトが表示されます。

```
Manager > ? (?は表示されません )

  Options : ACTivate ADD Connect CLear CREate DEACTivate DELete DESTroy
    DISable Disconnect DUMP EDit ENAble FINGer FLUsh Help LOAd MAIL MODify
    PING PURge REName Reconnect RESET RESTART SET SHow SSH STARt STop TELnet
    TRAce UPLoad LOGIN LOGON LOgoff LOgout

Manager >
```

表示されるキーワードのリストで、大文字の部分は省略形で、キーワードとして一意に識別するために最低限入力しなければなりません。

「SHOW」＋「半角スペース」を入力して、「?」キーを押すと、SHOW に続く選択可能なキーワードが表示され、プロンプトには「?」キーを押す寸前のコマンド（SHOW ＋半角スペース）が再表示されます。「?」を押すとき、コマンドラインに何らかの文字列を入力している場合、文字列の後ろに半角スペースを入力し、「?」と区切らなければなりません。

```
Manager > SHOW ? (?は表示されません )

  Options : ACC ALIas APPletalk BGP BOOTp BRIDge BRI BUFfer CLNS CONfig
    CPU DECnet DEBug DHCP DTe DTESt1 DVMrp ENCo ETH EXception FIle FEAture
    FIREwall FFIle FLash FRamerelay GRE GUI HTTP INSTall INTerface IP IPV6
    IPSec IPX ISAkmp ISDN L2TP LAPB LAPD LDAP LOAder LOG LPD MAnager MAIL
    MIOX NTP NVS OSPF PATch PERM PIM PING PKT ASYn POrt PKI PPP PRI Q931
    RADius RELease RSVP SA SCript SERvice SNmp SSH STAR STARTup STReam STT
    SWItch SYN SYStem TELnet TPAD TRAce TRIGger SESsions TCP TEST TIme TTy
    TACacs USEr VLAN VRRP X25C X25T TDM

Manager > SHOW
```

更に、選択可能なキーワードを掘り下げていく場合、例えば上記の例で「PPP」を指定する場合、続けて「PPP」＋「半角スペース」を入力し、「?」キーを押します。

```
Manager > SHOW PPP ? (?は表示されません)

  Options : COUnter CONFig MULTIlink IDLEtimer NAMEServers DEBUG TXSTatus
    TEMPlate LIMits PPPOE

Manager > SHOW PPP
```

コマンドの分割入力

CREATE、ADD で始まる長いコマンドは、CREATE と SET、ADD と SET の組み合わせを使って分割することができます。

例えば、CREATE で始まる下記の長いコマンドは、

```
Manager > CREATE PPP=0 OVER=eth0-any
    BAP=OFF IPREQUEST=ON
    USER="site_a@example.co.jp"
    PASSWORD="jK5H&2p"
    LQR=OFF ECHO=ON IDLE=ON ↵
```

図4.1.4 CREATE で始まる長いコマンド

次のように、CREATE と SET で始まる行に分割して入力することができます。この場合、「SET」コマンドでは先行して入力した「CREATE」コマンドのパラメーターを指定しなければなりません（下記では「ppp=0」や「over=eth0-any」）。

```
Manager > CREATE PPP=0 OVER=eth0-any
    BAP=OFF IPREQUEST=ON ↵

Manager > SET PPP=0
    USER="site_a@example.co.jp"
    PASSWORD="passwd_a" ↵

Manager > SET PPP=0 OVER=eth0-any
    LQR=OFF ECHO=ON IDLE=ON ↵
```

図4.1.5 CREATE、SET で分割

コマンドを分割して入力する際の各パラメータの指定等の詳細については、添付 CD-ROM 内の「コマンドリファレンス」にて参照できます。

IP フィルターコマンドの分割入力

コマンドが長くなりがちな IP フィルターコマンドについて、補足説明します。下記は、「ADD IP FILTER」コマンドがパラメーターとして取るおもなキーワードの省略形です。

ACTION:**AC**	DESTINATION:**DES**
DMASK:**DM**	DPORT:**DP**
ENTRY:**ENT**	EXCLUDE:**EXCL**
FILTER:**FIL**	INCLUDE:**INCL**
PROTOCOL:**PROT**	SESSION:**SESS**
SOURCE:**SO**	SMASK:**SM**
SPORT:**SP**	

また、SPORT、DPORT パラメーターには TELNET のようなプロトコル名を指定せずに、23 のようにポート番号を指定するとコマンド長が短縮できます。

コマンドリファレンス「IP」-「IP フィルター」-「ADD IP FILTER」

下記の長いコマンドは、

```
ADD IP FILTER=1 SOURCE=192.168.20.4
    SMASK=255.255.255.255
    DESTINATION=192.168.10.2
    DMASK=255.255.255.255 DPORT=TELNET
    PROTOCOL=TCP SESSION=ANY
    ACTION=INCLUDE
```

図 4.1.6 長いコマンド

次のように省略できます。

```
Manager > ADD IP FILT=1 SO=192.168.20.4
    SM=255.255.255.255 DES=192.168.10.2
    DM=255.255.255.255 DP=23
    PROT=TCP SESS=ANY AC=INCL ↵
```

図 4.1.7 省略形で入力

また、下記のコマンドは、

```
ADD IP FILTER=1 SOURCE=192.168.20.4
    SMASK=255.255.255.255
    DESTINATION=192.168.10.2
    DMASK=255.255.255.255 ACTION=INCLUDE
    ENTRY=1 DPORT=TELNET PROTOCOL=TCP
    SESSION=ANY
```

図 4.1.8 長いコマンド

ADD と SET の組み合わせを使い、コマンドを分割できます。「SET」コマンドでフィルター内容を追加する場合、必ず ENTRY パラメーターを指定してください。ENTRY はフィルタールール番号で、「SHOW IP FILTER」コマンドで確認できます。

```
Manager > ADD IP FILTER=1 SOURCE=192.168.20.4
    SMASK=255.255.255.255
    DESTINATION=192.168.10.2
    DMASK=255.255.255.255 ACTION=INCLUDE ↵

Manager > SHOW IP FILTER ↵

IP Filters
--------------------------------------------------------------------------------
No. Ent. Source Port   Source Address   Source Mask      Session           Size
         Dest. Port    Dest. Address    Dest. Mask       Prot.(T/C)     Options
         Type          Act/Pol/Pri      Logging                         Matches
--------------------------------------------------------------------------------
1    1   ---           192.168.20.4     255.255.255.255  ---                Any
         ---           192.168.10.2     255.255.255.255  Any                Any
         General       Include          Off                                   0

    Requests: 0            Passes: 0            Fails: 0
--------------------------------------------------------------------------------

Manager > SET IP FILTER=1 ENTRY=1
    DPORT=TELNET PROTOCOL=TCP
    SESSION=ANY ↵
```

図 4.1.9 ADD と SET で分割

4.2 コマンドの分類

本製品は、高度な機能を実現するために、多くのコマンド名やパラメーターをサポートしています。コマンドは、おおむね設定コマンドと、実行コマンドに分けることができます（コマンドによっては明確に分類できないものもあります）。

設定コマンド

設定コマンドは、「CREATE CONFIG」コマンドの実行により作成される設定スクリプトファイルの内容として保存されるか、または設定スクリプトファイルが保存されるとき、その内容に対して影響を与えます。*2

設定コマンドの多くは、ランタイムメモリー上に展開されている、本製品の動作を制御するための各種のテーブルの内容を変更します。例えば、「ADD IP ROUTE」コマンドは、ルーティングテーブルを変更し、パケットの配送を制御します。また、「PURGE IP」コマンドはIP に関するすべての設定を削除します。

設定コマンドは、内容によってはいくつかの設定コマンドを組み合わせて、はじめて有効となることもあります。代表的な設定コマンドには、以下のようなものがあります。

ACTIVATE
DEACTIVATE

「ACTIVATE」は、すでに存在しているものを実際に動作させるコマンドです。「DEACTIVATE」は、「ACTIVATE」コマンドで動作しているものを中止、または停止するコマンドです。例えば、設定済みの接続先に対する発呼や切断、スクリプトの実行や取りやめなどで使用します。

ADD
DELETE

「ADD」は、既存のテーブルなどに情報を追加、または登録するコマンドです。「DELETE」は、「ADD」で追加した情報を削除するコマンドです。例えば、インターフェースの追加や削除、ルーティング情報の追加や削除に使用します。

CREATE
DESTROY

「CREATE」は、存在していないものを作成するコマンドです*3。「DESTROY」は、「CREATE」で作成したものを削除するコマンドです。例えば、PPP インターフェースの作成や削除を行います。

ENABLE
DISABLE

「ENABLE」は、既存のものを有効化するコマンドです。「DISABLE」は、「ENABLE」で有効化したものを無効にするコマンドです。例えば、モジュールやインターフェースなどの有効化、無効化を行います。

PURGE

「PURGE」は、指定した項目を全消去するコマンドです。例えば、「PURGE USER」は、「manager/friend（デフォルト）」以外の、登録したユーザー情報をすべて削除します。

SET

「SET」は、すでに存在するパラメーターの設定、追加、または変更を行うコマンドです。「SET」が取るパラメーターによっては、「ADD」や「CREATE」コマンドの実行後でなければ、実行できないことがあります。

実行コマンド

実行コマンドは、「CREATE CONFIG」コマンドの実行により作成される設定スクリプトファイルの内容として保存されません。

実行コマンドは、ログイン、ログアウト、TELNET、ヘルプの表示、ファイルに対する操作、通信のテストなどのようなコマンドです。

実行コマンドを使用する前に、設定コマンドによってあらかじめ設定しなくてはならないこともあります。代表的な実行コマンドには、以下のようなものがあります。

EDIT

テキストエディターを起動するコマンドです。このコマンドにより、「.cfg」（設定スクリプトファイル）、「.scp」（スクリプトファイル）を直接編集することができます。

本書「6 テキストエディター」（p.55）

HELP

オンラインヘルプを表示するコマンドです。

本書「4.3 オンラインヘルプ」（p.39）

LOAD

TFTP サーバーや Zmodem などにより、ファイルを本製品にダウンロードするコマンドです。

本書「10 設定ファイルのバックアップとリストア」（p.65）

*2「SHOW CONFIG DYNAMIC」コマンドに対しても同様です。

*3 ある機能に対する設定コマンドが、ADD であるか、それとも CREATE であるかは、本製品における機能の実装に依存しています。

LOGIN

ログインするコマンドです。別のユーザーでログインしなおすときなどに使用します。

LOGOFF、LOGOUT

ログアウトするコマンドです。

本書「3.10 ログアウト」（p.32）

PING

指定した相手からの応答を確認するコマンドです。

本書「8.1 Ping」（p.59）

RESET

「RESET」は、設定内容は変更せずに、実行中の動作を中止し、はじめからやり直す（リセットする）コマンドです。

RESTART

本製品を再起動するコマンドです。

本書「3.9 再起動」（p.31）

SHOW

「SHOW」は、設定内容などの各種の情報を表示するコマンドです。

STOP PING

「PING」を中止するコマンドです。

本書「8.1 Ping」（p.59）

TELNET

「Telnet」を実行するコマンドです。

本書「7 Telnet を使う」（p.57）

TRACE

経路のトレースを実行するコマンドです。

本書「8.2 Trace」（p.59）

UPLOAD

TFTP サーバーや Zmodem などにより、ファイルをサーバーやコンピューターへアップロードするコマンドです。

本書「10 設定ファイルのバックアップとリストア」（p.65）

4.3 オンラインヘルプ

本製品は、オンラインヘルプを搭載しています。コマンドの概要や、コマンドが取り得るパラメーターとその範囲を知りたいときにご利用ください。オンラインヘルプは、ログイン後のプロンプトに対して使用できます。Manager レベル、User レベルでは表示されるヘルプの内容が異なります。

プロンプトに対して、「HELP」を入力すると、ヘルプのトップ画面が表示されます。

表示画面が 1 画面（24 行）におさまらない場合、「--MORE--」プロンプトが表示されます。「--MORE--」に対する操作キーは次の通りです。

- 「スペース」バーで、次の 1 ページを表示します。
- 「リターン」キーで、次の 1 行を表示します。
- 「C」キーで、該当項目の残りすべてを表示します。
- 「Q」キーで、表示を中止します。

```
Manager > HELP ↵

          AR570S オンラインヘルプ - V2.7 Rev.00 2005/11/01

 This online help is written in Japanese (Shift-JIS).

 ヘルプは次のトピックを説明しています。
 入力は大文字の部分だけでかまいません ("HELP OPERATION" は "H O"と省略可)。
 (# マーク付きの機能は追加ライセンスが必要です )

   Help Operation        運用・管理 (SNMP、ログ、トリガー、スクリプトなど)
   Help INterface        インターフェース (スイッチ、ETH、BRI、PRI など)
   Help ISdn             ISDN
   Help Tdm              専用線
   Help FRamerelay       フレームリレー
   Help PPp              PPP
   Help VLan             VLAN
   Help Bridge           ブリッジング
   Help IP               IP (RIP、OSPF、IPフィルターなど)
   Help IPV6             IPv6
   Help FIrewall         ファイアウォール
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

図 4.3.1 「HELP」の結果

トップ画面の内容から、さらに表示したい項目を指定します。ヘルプでも省略形が使用できます（大文字の部分が、最低限入力しなければならない文字列です）。例えば、「H O」を入力すると、運用・管理に関連するサブメニューが表示されます。

```
Manager > H O ↵

          AR570S オンラインヘルプ - V2.7 Rev.00 2005/11/01

運用・管理

    Help Operation SYstem                システム
    Help Operation Filesystem            記憶装置とファイルシステム
    Help Operation Configuration         コンフィグレーション
    Help Operation SHell                 コマンドプロセッサー
    Help Operation User                  ユーザー認証データベース
    Help Operation Authserver            認証サーバー
    Help Operation LOAder                アップロード・ダウンロード
    Help Operation Release               ソフトウェア
    Help Operation Mail                  メール送信
    Help Operation SEcurity              セキュリティー
    Help Operation LOG                   ログ
    Help Operation SCript                スクリプト
    Help Operation TRigger               トリガー
    Help Operation SNmp                  SNMP
    Help Operation Ntp                   NTP
--More--  (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

図4.3.2 「HELP OPERATION」の結果

更に項目を選択すると、該当項目のヘルプが表示されます。

```
Manager > H O SY ↵

          AR570S オンラインヘルプ - V2.7 Rev.00 2005/11/01

運用・管理 / システム

    DISABLE HTTP SERVER
    EDIT [filename]
    ENABLE HTTP SERVER
    HELP [topic]
    LOGIN [login-name]
    LOGOFF
    RESTART {REBOOT|ROUTER} [CONFIG={filename|NONE}]
    SET HELP=filename
    SET SYSTEM CONTACT=string
    SET SYSTEM DISTINGUISHEDNAME={dist-name|NONE}
    SET SYSTEM LOCATION=string
    SET SYSTEM NAME=string
    SET SYSTEM TERRITORY={AUSTRALIA|CHINA|EUROPE|JAPAN|KOREA|NEWZEALAND|
      USA}
    SET [TIME=time] [DATE=date]
--More--  (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

図4.3.3 「HELP OPERATION SYSTEM」の結果

4.4 インターフェース

物理インターフェース、データリンク層インターフェース、ネットワーク層インターフェースに関する概要を説明します。紙面の都合により、ISDN、専用線、フレームリレーには詳しく触れません。インターフェースに関する、完全な説明は下記をご覧ください。

コマンドリファレンス「インターフェース」-「概要」

インターフェースの階層構造

本製品の内部をソフトウェア的に見ると、下図のようになります。本製品に対する設定は、最下位に位置する物理インターフェースの上にさまざまな論理インターフェースを重ね、コマンドによって関連づけることによって行います。

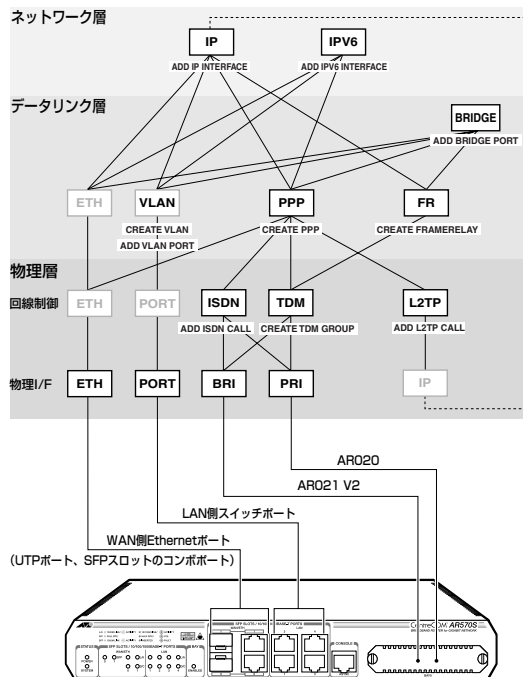



図4.4.1 インターフェースの階層構造

最下層は物理インターフェース（ポート）で、本製品に内蔵の LAN 側スイッチポート（PORT）、WAN 側 Ethernet ポート（ETH）、PIC ベイに装着するモジュールとして提供される PRI、BRI があります。

その上は、物理インターフェースに接続されている回線を制御するソフトウェアモジュールです。スイッチポート、Ethernet ポートの場

合は特に設定の必要がないため、明確な形では存在しません。BRI、PRIインターフェースでISDN網に接続するときは発信接続などを担当するISDNモジュールを、専用線やフレームリレー網に接続するときはタイムスロットの処理を行うTDMモジュールを使います。ここまでがOSIモデルでの物理層に相当します。

回線制御モジュールの上位にくるのが,OSI参照モデルの第2層にあたるデータリンク層インターフェースモジュールです。本製品ではVLAN、Ethernet、PPP、フレームリレー（FR）の4種類をサポートしています。この層では、単なるビット列をフレームと呼ばれる単位に組み立て、同一回線（データリンク）上での通信を制御します。Ethernetインターフェースは物理層とデータリンク層が一体となっているため、特に設定の必要はありません。LAN側スイッチポートは、ご購入時の状態で全ポートがvlan1（VLAN default）に所属していますが,VLANを追加作成することによって任意のグループに分割することができます。VLANの設定は、CREATE VLANコマンド、ADD VLAN PORTコマンドで行います。PPP、フレームリレーの場合は、「CREATE PPP」「CREATE FRAMERELAY」コマンドで明示的にインターフェースを作成します。このとき、下位インターフェースとして、回線制御モジュールか物理インターフェースを指定します。

データリンク層の上には、第3層にあたるネットワーク層プロトコルのインターフェースモジュールが位置します。本製品ではIP（IPv4）とIPv6をサポートしています。ネットワーク層インターフェースは、「ADD IP INTERFACE」「ADD IPV6 INTERFACE」コマンドを使って、データリンク層インターフェース上に追加（ADD）する形となります。

インターフェース名

インターフェース名は、インターフェースの種類を示す略称（ETH、PRIなど）に、インターフェース番号をつけたものです。本製品の物理インターフェースは、次のインターフェース名をもちます。

表4.4.1 物理インターフェース名

物理インターフェース	インターフェース名
LANスイッチポート	port1
	port2
	port3
	port4
WAN側Ethernetインターフェース（データリンク層と一体）	eth0
	eth1
BRIインターフェース（AR021 V2）	bri0
PRIインターフェース（AR020）	pri0

データリンク層（論理）インターフェースの番号は、「CREATE FRAMERELAY」、「CREATE PPP」、「CREATE VLAN」コマンドで指定した番号になります。番号は有効範囲内で任意に選べますが、通例として0から順に割り当てます[*4]。ただし、Ethernetは物理インターフェースの番号と同じとなります。

表4.4.2 データリンク層インターフェース名

インターフェース	名前の例
フレームリレーインターフェース	fr0など
PPPインターフェース	ppp0など
VLANインターフェース	vlan1など
WAB側Ethernetインターフェース（物理層と一体）	eth0、eth1

物理インターフェース

本製品で使用可能な物理インターフェースは、以下の4種類です。[*5]

- LAN側スイッチポート（port）
- WAN側Ethernetインターフェース（eth）
- BRIインターフェース（bri）
- PRIインターフェース（pri）

物理インターフェースは、本製品と各種回線を接続するための接続口（ポート）です。ソフトウェア的に見ると、ポートを制御するドライバーなどを含んでおり、上位の回線制御モジュールやデータリンク層インターフェースにサービスを提供します。

LAN側スイッチポート

本製品のLAN側は4ポートの10/100M/1000M Ethernetスイッチになっており、複数のコンピューターを接続することができます。これらのポートは、port1～port4（数字はポート番号）という名前で表します。

ご購入時の状態では、すべてのスイッチポートが「default」という名のVLAN（vlan1）に所属しているため、複数のVLANを必要としないのであれば、特にVLANの設定を意識する必要はありません。デフォルト状態のまま、LAN側スイッチ全体を

*4 コマンドで指定されたAR020、AR021 V2のインターフェース名「pri0」、「bri0」は、「SHOW CONFIG DYN」コマンドの表示や、「CREATE CONFIG」コマンドで作成された設定ファイルでは、「bay0.pri0」「bay0.bri0」のように変換されます。
また、「eth=0」、「pri=0」、「bri=0」のように指定されたパラメーターは、「eth=eth0」、「pri=bay0.pri0」、「bri=bay0.bri0」のように変換されます。

*5 本製品は、このほかに非同期シリアルインターフェース（asyn）1ポートを装備していますが、同ポートはコンソール接続専用となっております。モデムなどを接続してのネットワーク接続はサポートしておりません。

「vlan1」という名前のデータリンク層インターフェースとして扱うことができます。

LAN 側に対する上位層の設定（IP アドレスの割り当てなど）は、個々のスイッチポートではなく、スイッチポートを束ねた VLAN インターフェースに対して行います。

WAN 側 Ethernet インターフェース

WAN 側 Ethernet インターフェースは、本製品を Ethernet に接続するためのインターフェースです。本製品は、2 つのインターフェースを備えており、それぞれ「ETH0」、「ETH1」という名称を持っています。

このインターフェースを使用するにあたって、設定しなくてはならない項目はありません。他の物理インターフェースと異なり、Ethernet は物理層からデータリンク層（MAC 副層）までをカバーする規格であるため、直接上位にレイヤー3 インターフェース（IP、IPv6）を作成することができます。

また、このインターフェースは、Ethernet との接続だけでなく、PPPoE（PPP over Ethernet）による接続にも使用できます。PPPoE は Ethernet 上で PPP（Point-to-Point Protocol）を使用するためのプロトコルで、xDSL などのブロードバンドサービスで広く使用されています。

BRI インターフェース

BRI（Basic Rate Interface）インターフェースは、ITU-T が ISDN のユーザー・網インターフェースとして定めた I インターフェースのうち、基本インターフェース（I.430）と呼ばれる規格に準拠したインターフェースです。BRI は WAN 接続用のインターフェースで、ISDN 網（INS64。2B+ D）、専用線（64K、128K）、フレームリレー網との接続に使用できます。インターフェース名は「BRI0」です。

BRI インターフェースには、ISDN と専用線（TDM）の2 つの動作モードがあります。接続する回線に応じて動作モードを切り替えてください。動作モードの切り替えは「SET BRI」コマンドで行います。

PRI インターフェース

PRI（Primary Rate Interface）インターフェースは、ITU-T が ISDN のユーザー・網インターフェースとして定めた I インターフェースのうち、一次群インターフェース（I.431）と呼ばれる規格に準拠したインターフェースです。PRI は WAN 接続用のインターフェースで、ISDN 網（INS1500。23B +D）、専用線（192K ～ 1.5M）、フレームリレー網との接続に使用できます。インターフェース名は「PRI0」です。

PRI インターフェースには、ISDN と専用線（TDM）の2 つの動作モードがあります。接続する回線に応じて動作モードを切り替えてください。動作モードの切り替えは「SET PRI」コマンドで行います。

データリンク層インターフェース

本製品で使用できるデータリンク層インターフェースは以下の 4 種類です。

- VLAN インターフェース（vlan）
- WAN 側 Ethernet インターフェース（eth）
- PPP インターフェース（ppp）
- フレームリレーインターフェース（fr）

データリンク層インターフェースは、物理インターフェースの上に直接作成する場合と、物理インターフェース上にセットアップした回線制御モジュール上に作成する場合があります。以下、それぞれのセットアップ方法について、例を挙げながら簡単に説明します。

VLAN インターフェース

VLANインターフェースは、LAN側スイッチポートを束ねたデータリンク層インターフェースです。本製品は、設定により、LAN 側スイッチポートを任意のグループに分割できます。VLAN の種類としては、ポート VLAN とタグ VLAN（802.1Q）をサポートしています。

ご購入時の状態では、「default」という名前の VLAN（VID=1）が定義されており、すべてのスイッチポートがこの VLAN に所属しています。VLAN を複数必要としない限り、VLAN の設定を意識する必要はありません。この場合、LAN 側スイッチ全体を「vlan1」という名前のデータリンク層インターフェースとして扱うことができます。

VLAN インターフェースは、Ethernet インターフェースとほぼ同等のデータリンク層インターフェースとして使用できます。たとえば、vlan1（default）上に IP インターフェースを作成するには、次のようにします。

```
Manager > ADD IP INTERFACE=vlan1
    IP=192.168.10.1 MASK=255.255.255.0 ↵
```

VLAN 名を使って次のように書くこともできます。

```
Manager > ADD IP INTERFACE=vlan-default
    IP=192.168.10.1 MASK=255.255.255.0 ↵
```

注意

VLAN インターフェース上では、PPPoE を使用できません。

新たなVLANを作成する場合は、「CREATE VLAN」コマンドでVLANを作成し、「ADD VLAN PORT」コマンドでVLANにポートを割り当てます。

コマンドリファレンス「VLAN」-「概要」

WAN側Ethernetインターフェース

WAN側Ethernetインターフェースは、物理層とデータリンク層が一体になっています。このインターフェースを使用するにあたって特別な設定は必要ありません。ネットワーク層インターフェースの設定時に、インターフェース名（eth0、eth1）を指定するだけで使用できます。

PPPインターフェース

PPPインターフェースは、2点間のWAN接続に使用するデータリンク層インターフェースです。PPPインターフェースは、以下のインターフェース（物理インターフェースか回線制御モジュール）上に作成することができます。

- WAN側Ethernetインターフェース（eth）
- ISDNコール（ISDN接続）
- TDMグループ（専用線接続）

また、トンネリングプロトコルL2TPを使用すると、IPネットワーク上に仮想的な回線（L2TPコール）を構築し、その上にPPPインターフェースを作成することもできます。

PPPインターフェースは「CREATE PPP」コマンドで作成します。下位のインターフェースは、OVERパラメーターで指定します。

Ethernet上でPPPを使用する（PPP over Ethernet。PPPoE）には、OVERパラメーターに「Ethernetインターフェース名」＋ハイフン（-）＋「PPPoEサービス名」を指定します。プロバイダーからPPPoEサービス名が指定されていない場合は、すべてのサービスを意味するキーワード「any」か任意の文字列を指定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵
```

ISDN上でPPPを使用するには、OVERパラメーターにISDNコール名を「ISDN-」＋「コール名」の形式で指定します。ISDN回線では、通常「IDLE=ON」を指定してダイヤルオンデマンドを有効にします。

```
Manager > CREATE PPP=0 OVER=ISDN-remote
    IDLE=ON ↵
```

BRI、PRIインターフェースによる専用線接続でPPPを使用するには、OVERパラメーターにTDMグループ名を「TDM-」＋「グループ名」の形式で指定します。

```
Manager > CREATE PPP=0 OVER=TDM-remote ↵
```

コマンドリファレンス「PPP」-「概要」

フレームリレーインターフェース

フレームリレー（FR）インターフェースは、フレームリレー網と接続するときに使うデータリンク層インターフェースです。FRインターフェースは、TDMグループ（専用線接続）上に作成することができます。

FRインターフェースは、「CREATE FRAMERELAY」コマンドで作成します。下位のインターフェースは、OVERパラメーターで指定します。

BRI、PRIインターフェースでフレームリレー網に接続するときは、「CREATE FRAMERELAY」コマンドのOVERパラメーターに、TDMグループ名を「TDM-」＋「グループ名」の形式で指定します。また、使用するPVC状態確認手順（LMI）をLMISCHEMEパラメーターで指定してください。「RESET FR=0」はLMIの設定を有効にするためのコマンドです。

```
Manager > CREATE FR=0 OVER=TDM-remote LMIS-
    CHEME=ANNEXD ↵
Manager > RESET FR=0 ↵
```

コマンドリファレンス「フレームリレー」-「概要」

ネットワーク層インターフェース

本製品で使用できるネットワーク層インターフェースは以下の2種類です。

- IPインターフェース
- IPv6インターフェース

ネットワーク層インターフェースは、本製品の基本機能であるルーティングのためのインターフェースです。本製品をルーターとして機能させるためには、使用するルーティングモジュール（IP、IPv6）を有効にし、ネットワーク層インターフェースを2つ以上作成する必要があります。

ネットワーク層インターフェースは、データリンク層インターフェースの上に作成します。

IP インターフェース

IP インターフェースは、IP パケットの送受信を行うためのインターフェースです。IP モジュールを有効にし、IP インターフェースを複数作成した時点で IP パケットの転送（ルーティング）が行われるようになります。

IP インターフェースは、「ADD IP INTERFACE」コマンドでデータリンク層インターフェースに IP アドレス（とネットマスク）を割り当てることによって作成します。

作成したIPインターフェースは、データリンク層インターフェースと同じ名前で参照できます。例えば、Ethernet インターフェース「0」上に作成した IP インターフェースを他の IP 関連コマンドで指定するときは「eth0」とします。

IP モジュールを有効化するには、「ENABLE IP」コマンドを実行します。

```
Manager > ENABLE IP ↵
```

VLAN インターフェースに IP アドレスを設定するには次のようにします。

```
Manager > ADD IP INT=VLAN1 IP=192.168.1.1
    MASK=255.255.255.0 ↵
```

Ethernet インターフェースに IP アドレスを設定するには次のようにします。

```
Manager > ADD IP INT=ETH0 IP=192.168.10.1
    MASK=255.255.255.0 ↵

Manager > SHOW IP INTERFACE ↵

Interface     Type      IP Address        Bc Fr PArp  Filt RIP Met.   SAMode  IPSc
Pri. Filt     Pol.Filt Network Mask      MTU   VJC   GRE  OSPF Met.  DBcast  Mul.
-------------------------------------------------------------------------------
Local         ---       Not set           -  -  -     ---  --         Pass    --
---           ---       Not set           1500  -     ---  --         ---     ---
vlan1         Static    192.168.1.1       1  n  Off   ---  01         Pass    No
---           ---       255.255.255.0     1500  -     ---  0000000001 No      Rec
eth0          Static    192.168.10.1      1  n  On    ---  01         Pass    No
---           ---       255.255.255.0     1500  -     ---  0000000001 No      Rec
-------------------------------------------------------------------------------
```

PPPインターフェースに IPアドレスを設定するには次のようにします。

```
Manager > ADD IP INT=PPP0 IP=192.168.100.1
    MASK=255.255.255.0 ↵
```

マルチホーミング

ひとつのデータリンク層インターフェースに対して、複数の IP インターフェース（IP アドレス）を与えることを「マルチホーミング」と言います。本製品では、データリンク層インターフェースに対して、最大 16 個までの IP インターフェースを持たせることができます。

マルチホーミングされたインターフェース名は、「eth0-1」のようにインターフェース名の後に、ハイフンで 0 〜 15 番号の番号を付けて表します。マルチホーミングすると、例えば「eth0」は「eth0-0」と表示されます。

VLAN1 に 192.168.1.1 を割り当てるとします。

```
Manager > ENABLE IP ↵

Info (1005287): IP module has been enabled.

Manager > ADD IP INT=VLAN1 IP=192.168.1.1 ↵

Info (1005275): interface successfully added.

Manager > SHOW CONFIG DYN=IP ↵

#
# IP configuration
#
enable ip
add ip int=vlan1 ip=192.168.1.1
```

次に、VLAN1-1 に 192.168.2.1 を割り当てるとすると、VLAN1 は VLAN1-0 となります。

```
Manager > ADD IP INT=VLAN1-1 IP=192.168.2.1 ↵

Info (1005275): interface successfully added.

Manager > SHOW CONFIG DYN=IP ↵

#
# IP configuration
#
enable ip
add ip int=vlan1-0 ip=192.168.1.1
add ip int=vlan1-1 ip=192.168.2.1
```

4.5 ルーティング（スタティック）

2 つの LAN の接続

ネットワークX と Y があり、X と Y をルーターで接続するには、以下のように設定します。

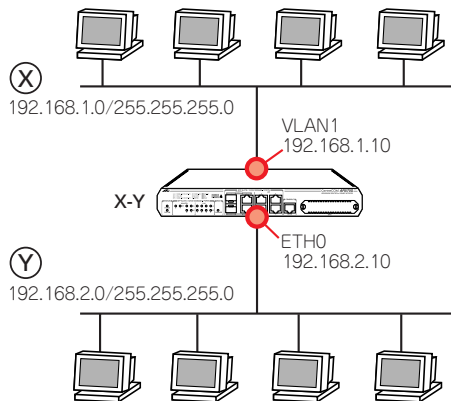



図4.5.1 2 つの LAN の接続

1 ルーターX-Y に、Manager レベルでログインします。

```
login:manager ↵
Password:friend ↵
```

2 わかりやすさのために、システム名を設定します。

```
Manager > SET SYSTEM NAME=X-Y ↵

Info (134003): Operation successful.

Manager X-Y>
```

3 IP モジュールを有効にします。

```
Manager X-Y> ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

4 物理インターフェースにIP アドレスを設定します。
VLAN1 に対して、下記を入力します。

```
Manager X-Y> ADD IP INTERFACE=vlan1
    IP=192.168.1.10 MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

ETH0 に対して、下記を入力します。

```
Manager X-Y> ADD IP INTERFACE=eth0
    IP=192.168.2.10 MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.

Manager > SHOW IP INTERFACE ↵

Interface    Type     IP Address       Bc Fr PArp  Filt RIP Met.   SAMode IPSc
Pri. Filt    Pol.Filt Network Mask     MTU   VJC   GRE  OSPF Met.  DBcast Mul.
------------------------------------------------------------------------------
Local        ---      Not set          -  -  -     ---  --         Pass   --
---          ---      Not set          1500  -     ---  --         ---    ---
vlan1        Static   192.168.1.10     1  n  Off   ---  01         Pass   No
---          ---      255.255.255.0    1500  -     ---  0000000001 No     Rec
eth0         Static   192.168.2.10     1  n  On    ---  01         Pass   No
---          ---      255.255.255.0    1500  -     ---  0000000001 No     Rec
------------------------------------------------------------------------------
```

5 物理インターフェースに IP アドレスを割り当てると、それらのアドレスはルーティングテーブルに登録され、ネットワーク X と Y は通信可能となります。下記は、各ネットワークが物理インターフェースに直接接続されていることを示しています。

```
Manager X-Y> SHOW IP ROUTE ↵

IP Routes
--------------------------------------------------------------------------
Destination     Mask                NextHop              Interface        Age
DLCI/Circ.      Type      Policy    Protocol             Metrics   Preference
--------------------------------------------------------------------------
192.168.1.0     255.255.255.0       0.0.0.0              vlan1             16
-               direct    0         interface            1                  0
192.168.2.0     255.255.255.0       0.0.0.0              eth0               7
-               direct    0         interface            1                  0
--------------------------------------------------------------------------
```

3 つの LAN の接続

図 4.5.1（p.45）の例に、ネットワーク Z を追加する場合は、以下のように設定します。

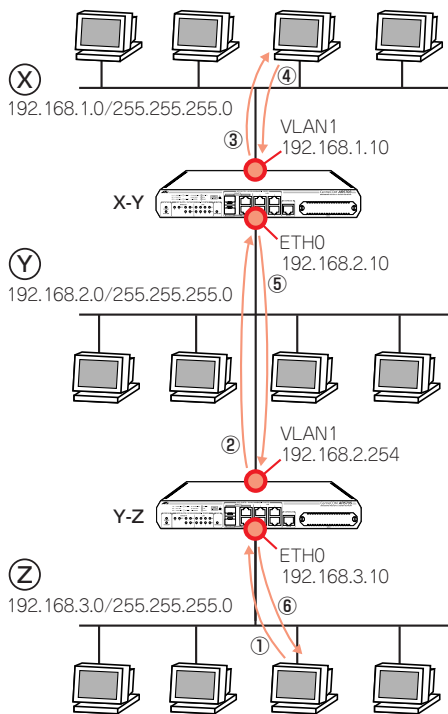



図4.5.2 3 つの LAN の接続

1 ルーターY-Z に、Manager レベルでログインします。

```
login:manager ↵
Password:friend ↵
```

2 わかりやすさのために、システム名を設定します。

```
Manager > SET SYSTEM NAME=Y-Z ↵

Info (134003): Operation successful.

Manager Y-Z>
```

3 IP モジュールを有効にします。

```
Manager Y-Z> ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

4 物理インターフェースにIP アドレスを設定します。
VLAN1 に対して、下記を入力します。

```
Manager Y-Z> ADD IP INTERFACE=vlan1
    IP=192.168.2.254 MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

ETH0 に対して、下記を入力します。

```
Manager Y-Z> ADD IP INTERFACE=eth0
    IP=192.168.3.10 MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

5 物理インターフェースに IP アドレスを割り当てると、それらのアドレスはルーティング情報として ,ルーティングテーブルに登録され、ネットワーク Y と Z は通信可能となります。下記は、各ネットワークが物理インターフェースに直接接続されていることを示しています。

```
Manager Y-Z> SHOW IP ROUTE ↵

IP Routes
--------------------------------------------------------------------------------
Destination      Mask             NextHop          Interface          Age
DLCI/Circ.       Type     Policy  Protocol         Metrics            Preference
--------------------------------------------------------------------------------
192.168.2.0      255.255.255.0    0.0.0.0          vlan1              15
-                direct    0      interface        1                  0
192.168.3.0      255.255.255.0    0.0.0.0          eth0               6
-                direct    0      interface        1                  0
--------------------------------------------------------------------------------
```

6 しかしながら、X-Y はネットワーク Z の所在を知らないため、X から Z に向かうパケットを配送できません。また、Y-Z はネットワーク X の所在を知らないため、Z から X に向かうパケットを配送できません。X と Z 間の通信ができるようにするために、「ADD IP ROUTE」コマンドにより、ネットワークの所在（経路情報）をルーティングテーブルに登録します。

X-Y に対して、ネットワーク Z（192.168.3.0）は、ETH0 に接続されている側のネットワークの 192.168.2.254 にパケットを送ればよいことを教えてやります。METRIC は、経由するルー

ターの数＋１を設定します。

```
Manager X-Y> ADD IP ROUTE=192.168.3.0
    MASK=255.255.255.0 INTERFACE=eth0
    NEXTHOP=192.168.2.254 METRIC=2 ↵

Info (1005275): IP route successfully added.
```

X-Y のルーティングテーブルは、次のようになります。

```
Manager X-Y> SHOW IP ROUTE ↵

IP Routes
--------------------------------------------------------------------------------
Destination      Mask             NextHop          Interface         Age
DLCI/Circ.       Type    Policy   Protocol         Metrics           Preference
--------------------------------------------------------------------------------
192.168.1.0      255.255.255.0    0.0.0.0          vlan1             107
-                direct   0       interface        1                 0
192.168.2.0      255.255.255.0    0.0.0.0          eth0              97
-                direct   0       interface        1                 0
192.168.3.0      255.255.255.0    192.168.2.254    eth0              5
-                remote   0       static           2                 60
--------------------------------------------------------------------------------
```

Y-Z に対して、ネットワーク X（192.168.1.0）は、VLAN1 に接続されている側のネットワークの192.168.2.10にパケットを送ればよいことを教えてやります。METRIC は、経由するルーターの数＋１を設定します。

```
Manager Y-Z> ADD IP ROUTE=192.168.1.0
    MASK=255.255.255.0 INTERFACE=vlan1
    NEXTHOP=192.168.2.10 METRIC=2 ↵

Info (1005275): IP route successfully added.
```

Y-Z のルーティングテーブルは、次のようになります。

```
Manager Y-Z> SHOW IP ROUTE ↵

IP Routes
--------------------------------------------------------------------------------
Destination      Mask             NextHop          Interface         Age
DLCI/Circ.       Type    Policy   Protocol         Metrics           Preference
--------------------------------------------------------------------------------
192.168.1.0      255.255.255.0    192.168.2.10     vlan1             9
-                remote   0       static           2                 60
192.168.2.0      255.255.255.0    0.0.0.0          vlan1             517
-                direct   0       interface        1                 0
192.168.3.0      255.255.255.0    0.0.0.0          eth0              508
-                direct   0       interface        1                 0
--------------------------------------------------------------------------------
```

7 以上で、ネットワークX、Y、Z は相互に通信できるようになります。

デフォルトルート

ネットワークX、Y、Z をインターネットに接続する場合は、デフォルトルートを設定します。デフォルトルートとは、最終到達点までの経路が不明なパケットを配送してくれるルーターまでの経路です。以下の例では、インターネットに向かうパケット、すなわち X、Y、Z 以外のアドレスを持つパケットを配送してくれるルーターまでの経路です。

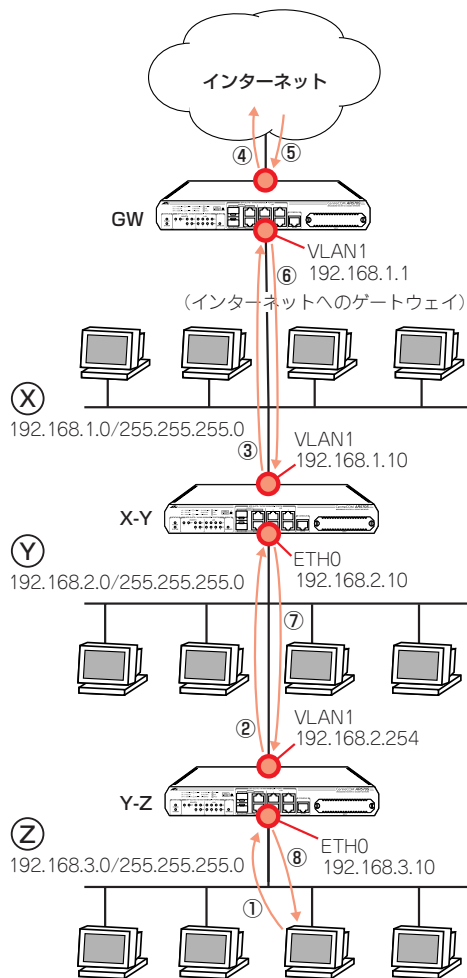



図 4.5.3 インターネットにも接続

1 X-Yに対して、インターネットに向かう任意のパケットは、VLAN1に接続されている側のネットワークの 192.168.1.1 に送ればよいことを教えてやります。

```
Manager X-Y> ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0
    INTERFACE=vlan1 NEXTHOP=192.168.1.1
    METRIC=2 ↵

Info (1005275): IP route successfully added.
```

X-Yのルーティングテーブルは、次のようになります。

```
Manager X-Y> SHOW IP ROUTE ↵

IP Routes
--------------------------------------------------------------------------------
Destination      Mask               NextHop             Interface          Age
DLCI/Circ.       Type     Policy    Protocol            Metrics     Preference
--------------------------------------------------------------------------------
0.0.0.0          0.0.0.0            192.168.1.1         vlan1                6
-                remote   0         static              2                  360
192.168.1.0      255.255.255.0      0.0.0.0             vlan1             3488
-                direct   0         interface           1                    0
192.168.2.0      255.255.255.0      0.0.0.0             eth0              3478
-                direct   0         interface           1                    0
192.168.3.0      255.255.255.0      192.168.2.254       eth0              3386
-                remote   0         static              2                   60
--------------------------------------------------------------------------------
```

2 Y-Zに対して、インターネットに向かう任意のパケットは、VLAN1が接続されている側のネットワークの 192.168.2.10に送ればよいことを教えてやります。METRIC は、経由するルーターの数＋1を設定します。

```
Manager Y-Z> ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0
    INTERFACE=vlan1 NEXTHOP=192.168.2.10
    METRIC=2 ↵

Info (1005275): IP route successfully added.
```

Y-Zのルーティングテーブルは、次のようになります。

```
Manager Y-Z> SHOW IP ROUTE ↵

IP Routes
--------------------------------------------------------------------------------
Destination      Mask               NextHop             Interface          Age
DLCI/Circ.       Type     Policy    Protocol            Metrics     Preference
--------------------------------------------------------------------------------
0.0.0.0          0.0.0.0            192.168.2.10        vlan1                3
-                remote   0         static              2                  360
192.168.1.0      255.255.255.0      192.168.2.10        vlan1              151
-                remote   0         static              2                   60
192.168.2.0      255.255.255.0      0.0.0.0             vlan1              181
-                direct   0         interface           1                    0
192.168.3.0      255.255.255.0      0.0.0.0             eth0               172
-                direct   0         interface           1                    0
--------------------------------------------------------------------------------
```

この場合、宛先がネットワーク X のパケットは、デフォルトルートによっても配送が可能なので、手順6（p.46）の下記のコマンドは省略できます。

```
Manager Y-Z> ADD IP ROUTE=192.168.1.0
    MASK=255.255.255.0 INTERFACE=vlan1
    NEXTHOP=192.168.2.10 METRIC=2 ↵

Info (1005275): IP route successfully added.
```

インターネットからの戻りのルート

ゲートウェイ GW には、インターネットからの戻りのパケットが、ネットワーク Y、Z に配送されるよう、経路情報を追加する必要があります。

```
Manager GW> ADD IP ROUTE=192.168.2.0
    MASK=255.255.255.0 INTERFACE=vlan1
    NEXTHOP=192.168.1.10 METRIC=2 ↵

Manager GW> ADD IP ROUTE=192.168.3.0
    MASK=255.255.255.0 INTERFACE=vlan1
    NEXTHOP=192.168.1.10 METRIC=2 ↵
```

コンピューターにおけるデフォルトルート

ネットワーク X、Y には、ルーターが 2 つずつあります。各ネットワークのコンピューターに設定するデフォルトゲートウェイ[*6] は、2 つのルーターのどちらを指定してもかまいません。例えば、デフォルトゲートウェイとして 192.168.2.10 が設定された、ネットワーク Y のコンピューターがネットワーク Z と通信する場合、コンピューターからのパケットはルーターX-Y に向かって送信されますが、そのパケットは X-Y によって Y-Z に転送されます。

*6 コンピューターでは、直接接続されていないネットワーク宛のパケットのすべては、デフォルトゲートウェイ（デフォルトルート）に送ります。

5.1 ユーザーレベル

権限によって、User（一般ユーザー）、Manager（管理者）、Security Officer（保安管理者）の３つのユーザーレベルが存在します。

表5.1.1：動作 モードとユーザーレベルの権限

レベル	ノーマルモード	セキュリティーモード
User	• ユーザー自身に関する端末設定、パスワードのようなごく一部のコマンドのみ実行可能 • おもにWAN を経由で接続してくるPPP ユーザーの認証に使用	
Manager	• すべてのコマンドを実行可能	• ユーザーや IPsec などセキュリティーに関するコマンドの実行不可 • 第 2 位のユーザーレベル
Security Officer	• すべてのコマンドを実行可能 • Manager と同じユーザーレベル	• すべてのコマンドを実行可能 • 第 1 位のユーザーレベル

Manager、Security Officer レベルの権限は、動作モードによって変わります。

 本書「5.4 ノーマルモード / セキュリティーモード」（p.52）

ユーザーレベルによって、コマンドプロンプトが変わります。

 本書「4.1 コマンドプロセッサー」（p.35）

5.2 ユーザー認証データベース

本製品は、ユーザー認証データベースを持っており、次のような状況が発生したとき、このデータベースを使用してユーザーの認証を行います。

- コンソールターミナルまたは Telnet によってユーザーが本製品にログインするとき
- PPP によって相手が接続してきたとき

関連する情報として、本書「3.4 パスワードの変更」（p.28）、「4.1 コマンドプロセッサー」（p.35）もご覧ください。

ユーザー認証データベースには、次のような情報を登録することができます。このデータベースへのアクセスは、ノーマルモードでは Manager または Security Officer レベル、セキュリティーモードではSecurity Officer レベルの権限が必要です。

表5.2.1 ユーザー認証データベース

ユーザー名	USER • 1～64文字の半角のアルファベットと数字を使用可 • スペース、「?」、ダブルクォーテーション「"」は使用不可。その他の半角記号は使用可 • 大文字、小文字の区別なし
パスワード	PASSWORD • 1～32文字までの半角のアルファベットと数字を使用可 • デフォルトでは 6 文字以上の長さが必要 • 「?」、ダブルクォーテーション「"」は使用不可。その他の半角記号は使用可 • スペースが含まれる場合、ダブルクォーテーション「"」でくくる • 大文字、小文字の区別あり
ユーザーレベル	PRIVILEGE • USER、MANAGER、SECURITYOFFICER から選択 • デフォルトのユーザーレベルは「USER」
ログイン権	LOGIN • コンソールターミナルまたは Telnet によるログインを許可するか否か • ユーザーレベルが「USER」の場合は必須。USER レベルのユーザーは、おもに PPP の認証に使用されるものなので、通常は「LOGIN=NO」を指定
Telnet 実行権	TELNET • ログインしたユーザーに TELNET コマンドの実行権を与えるか否か • デフォルトは「与えない」
コメント	DESCRIPTION • ユーザーについての説明

ご購入時には、Manager レベルのユーザー「manager」のみが登録されています。初期パスワードは「friend」です。

 本書「3.3 ログイン（ご購入時）」（p.28）

ユーザー認証データベースだけでなく、RADIUS サーバーによる認証も可能です。

 コマンドリファレンス「運用・管理」-「ユーザー認証データベース」-「ユーザー認証処理の順序」
コマンドリファレンス「運用・管理」-「認証サーバー」

5.3 ユーザーの登録と情報の変更

ユーザー認証データベースへのアクセスは、ノーマルモードでは Manager レベル、セキュリティーモードでは Security Officer レベルの権限が必要です。

新規ユーザー登録

1 Managerレベルでログインします。下記では、ユーザー「manager」ログインしています。

```
 login: manager ↲
Password: ________  （表示されません）

Manager > ADD USER=osaka-shisya
    PASSWORD="okonomiyaki" LOGIN=NO ↲
```

2 新規ユーザー登録は、「ADD USER」コマンドを使います。下記では、ユーザー名「osaka-shisya」、パスワード「okonomiyaki」を仮定しています。ユーザーレベルは User です（デフォルト）。ユーザーレベルが「User」であるため、LOGIN パラメーターの指定が必要です。PPP 認証のためのユーザーなので「NO」を指定します。「TELNET」コマンドは使用できません（デフォルト）。

```
Manager > ADD USER=osaka-shisya
    PASSWORD="okonomiyaki" LOGIN=NO ↲
```

Manager レベルでログインすると、セキュリティータイマーがスタートします（デフォルトは 60 秒）。ログインして 60 秒以内にユーザー管理コマンドを実行した場合、パスワードは要求されませんが、60 秒以上経過すると Manager レベルのパスワードを要求されます。

```
This is a security command, enter your password at the prompt
Password: ________  （表示されません）

User Authentication Database
----------------------------------------------------------------------------
Username: osaka-shisya ()
   Status: enabled    Privilege: user      Telnet: no    Login: no
   Logins: 0          Fails: 0        Sent: 0           Rcvd: 0
   Authentications: 0 Fails: 0
----------------------------------------------------------------------------
```

タイマーはユーザー管理コマンドを実行するたびにリセットされます。60 秒以内にユーザー管理コマンドを実行しないとタイマーがタイムアウトし、あらためて Manager レベルのパスワードを要求されます。

セキュリティータイマーの値は、次のコマンドで変更できます。下記は、90 秒に変更しています。値は 10 ～600 秒に設定できます。

```
Manager > SET USER SECUREDELAY=90 ↲

This is a security command, enter your password at the prompt
Password: ________  （表示されません）

User module configuration and counters
---------------------------------------------------------------------------
Security parameters
  login failures before lockout ...........     5            (LOGINFAIL)
  lockout period ..........................   600 seconds    (LOCKOUTPD)
  manager password failures before logoff ..    3            (MANPWDFAIL)
  maximum security command interval ........   90 seconds    (SECURDELAY)
  minimum password length .................     6 characters (MINPWDLEN)
  TACACS retries ..........................     3            (TACRETRIES)
  TACACS timeout period ...................     5 seconds    (TACTIMEOUT)
  semi-permanent manager port ............. none

Security counters
  logins                      2     authentications              0
  managerPwdChanges           0     defaultAcctRecoveries        1
  unknownLoginNames           0     tacacsLoginReqs              0
  totalPwdFails               0     tacacsLoginRejs              0
  managerPwdFails             0     tacacsReqTimeouts            0
  securityCmdLogoffs          0     tacacsReqFails               0
  loginLockouts               0     databaseClearTotallys        0
---------------------------------------------------------------------------
```

ユーザー情報変更

既に登録されているユーザーの情報を変更する場合、「SET USER」コマンドを使用します。下記では、「osaka-shisya」にログイン権限を与え、コメントを追加しています。

```
Manager > SET USER=osaka-shisya LOGIN=yes
    DESC="osaka-shisya PPP account" ↲

This is a security command, enter your password at the prompt
Password: ________  （表示されません）

User Authentication Database
----------------------------------------------------------------------------
Username: osaka-shisya (osaka-shisya PPP account)
   Status: enabled    Privilege: user      Telnet: no    Login: yes
   Logins: 0          Fails: 0        Sent: 0           Rcvd: 0
   Authentications: 0 Fails: 0
----------------------------------------------------------------------------
```

パスワード変更

ユーザー本人がパスワードを変更する場合は、「SET PASSWORD」コマンドを使用します（この場合、パスワードにスペースを含んでもダブルクオートでくくる必要はありません）。

```
 login: osaka-shisya ↵
Password:

> SET PASSWORD ↵

OLD passsowd: ________  （表示されません）
New password: ________  （表示されません）
Confirm: ________  （表示されません）
```

本書「3.4 パスワードの変更」（p.28）

ユーザー「manager」のパスワードを変更した場合、パスワードを忘れないでください。パスワードを忘れると、本製品にログインできなくなりますので、充分にご注意ください。

ユーザー情報表示

ユーザー情報の表示は、「SHOW USER」コマンドを使います。

```
Manager > SHOW USER ↵

User Authentication Database
---------------------------------------------------------------------------
Username: manager (Manager Account)
   Status: enabled    Privilege: manager   Telnet: yes   Login: yes
   Logins: 4          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
Username: osaka-shisya (osaka-shisya PPP account)
   Status: enabled    Privilege: user      Telnet: no    Login: yes
   Logins: 0          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
---------------------------------------------------------------------------


Active (logged in) Users
------------------------

User            Port/Device
    Login Time               Location
----------------------------------------------------------------------
manager         Asyn 0
    15:52:20 26-Mar-2005     local
----------------------------------------------------------------------
```

ユーザー削除

ユーザーの削除は、「DELETE USER」コマンドを使います。

```
Manager > DELETE USER=osaka-shisya ↵

This is a security command, enter your password at the prompt
Password: ________  （表示されません）

Info (145265): DELETE USER, user osaka-shisya has been deleted.
```

ユーザー一括削除

全ユーザーの一括削除は、「PURGE USER」コマンドを使います。ご購入時における唯一のユーザー「manager」は削除されませんが、パスワードを変更している場合、ご購入時の「friend」に戻ります。

```
Manager > PURGE USER ↵

This is a security command, enter your password at the prompt
Password: ________  （表示されません）

Info (145269): PURGE USER, user database has been purged.

Manager > SHOW USER ↵

---------------------------------------------------------------------------
Username: manager (Manager Account)
   Status: enabled    Privilege: manager   Telnet: yes   Login: yes
   Logins: 0          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
---------------------------------------------------------------------------
```

5.4 ノーマルモード / セキュリティーモード

本製品は、「ノーマルモード」「セキュリティーモード」の 2 つの動作モードを持っています。

ノーマルモード（Normal Mode）

デフォルトの動作モードです。ご購入時は、このモードとなっています。

セキュリティーモード（Security Mode）

より高いセキュリティーレベルを実現するためのモードです。ログインセキュリティーや管理コマンドの実行権が厳しく制限されます。

IPsecなどのセキュリティー機能を利用するときや、本製品の管理に関するセキュリティーを高めたい場合に使います。

セキュリティーモードへの移行

セキュリティーモードに移行するためには、あらかじめ Security Officer レベルのユーザーを作成しておく必要があります。セキュリティーモードに移行すると、Manager レベルは第 2 位の権限レベルに降格され、セキュリティーに関するコマンドを実行できなくなります。

1 Security Officer レベルのユーザーを作成します。

```
Manager > ADD USER=secoff
    PRIVILEGE=SECURITYOFFICER
    PASSWORD="top secret" ↵
```

2 セキュリティーモードに移行すると、Telnet 接続では Security Officer レベルでログインできなくなるので（他のレベルならログイン可）、必要に応じて RSO（Remote Security Officer）の設定をしておきます。

```
Manager > ENABLE USER RSO ↵

This is a security command, enter your password at the prompt
Password:_________  （表示されません）

Info (1045057): RSO has been enabled.

Manager > ADD USER RSO IP=192.168.1.100 ↵

Remote Security Officer Access is enabled

Remote Security Officer ... 192.168.1.100/255.255.255.255
```

RSO は、セキュリティーモードにおいて、指定したアドレスからのSecurity Officer レベルでのログインを許可する機能です。

3 Security Officer レベルのアカウントを設定スクリプトとして保存し、起動時に実行されるように指定しておきます。

```
Manager > CREATE CONFIG=TEST01.CFG ↵

Info (1034003): Operation successful.

Manager > SET CONFIG=TEST01.CFG ↵

Info (1034003): Operation successful.
```

4 セキュリティーモードに移行するには「ENABLE SYSTEM SECURITY_MODE」コマンドを実行します。

```
Manager > ENABLE SYSTEM SECURITY_MODE ↵

Info (1034003): Operation successful.
```

このコマンドを実行すると、フラッシュメモリーに「enabled.sec」ファイルが作成されます。システム起動時に本ファイルが存在すればセキュリティーモードとなります。このファイルを削除したり、修正、編集、コピー、リネームなどを行わないでください。

5 Security Officer レベルでログインしなおすと、コマンドプロンプトが「SecOff >」に変わります。

```
Manager > LOGIN secoff ↵

Password: _________  （表示されません）

SecOff >
```

6 Security Officer レベルでログインすると、セキュリティータイマーがスタートします（デフォルトは 60 秒）。ログインして 60 秒以内にセキュリティーに関連するコマンドを実行した場合、パスワードは要求されませんが、60 秒以上経過すると、Security Officer レベルのパスワードを要求されます。

```
SecOff > add user=nagoya-sisya
    password="misokatsu" login=no ↵

This is a security command, enter your password at the prompt
Password: _________  （表示されません）

Number of logged in Security Officers currently active.....1

User Authentication Database
--------------------------------------------------------------------------------
Username: nagoya-sisya ()
   Status: enabled    Privilege: user      Telnet: no     Login: no
   Logins: 0          Fails: 0        Sent: 0           Rcvd: 0
   Authentications: 0 Fails: 0
--------------------------------------------------------------------------------
```

タイマーはセキュリティー関連コマンドを実行するたびにリセットされます。60 秒以内にセキュリティーコマンドを実行し

ないとタイマーがタイムアウトし、ログインユーザーの権限はManager レベルに格下げされます。格下げされた状態でセキュリティーコマンドを実行しようとすると、あらためて Security Officer レベルのパスワードを要求されます。

セキュリティータイマーの値は、次のコマンドで変更できます。下記は、90 秒に変更しています。値は 10 〜 600 秒に設定できます。

```
SecOff > SET USER SECUREDELAY=90 ↵

This is a security command, enter your password at the prompt
Password: _________   (表示されません)

User module configuration and counters
--------------------------------------------------------------------------------
Security parameters
  login failures before lockout ...........     5            (LOGINFAIL)
  lockout period ..........................   600 seconds    (LOCKOUTPD)
  manager password failures before logoff ..    3            (MANPWDFAIL)
  maximum security command interval ........   90 seconds    (SECURDELAY)
  minimum password length .................     6 characters (MINPWDLEN)
  TACACS retries ..........................     3            (TACRETRIES)
  TACACS timeout period ...................     5 seconds    (TACTIMEOUT)
  semi-permanent manager port ............. none

Security counters
  logins                       5     authentications              0
  managerPwdChanges            0     defaultAcctRecoveries        2
  unknownLoginNames            0     tacacsLoginReqs              0
  totalPwdFails                2     tacacsLoginRejs              0
  managerPwdFails              0     tacacsReqTimeouts            0
  securityCmdLogoffs           0     tacacsReqFails               0
  loginLockouts                0     databaseClearTotallys        1
--------------------------------------------------------------------------------
```

現在の動作モードを確認するには「SHOW SYSTEM」コマンドを実行します。「Security Mode」が Enabled ならセキュリティーモード、Disabledならノーマルモードです。

セキュリティーモード時に「SET CONFIG」コマンドで起動スクリプトを変更するときは注意が必要です。例えば、SET CONFIG=NONE を実行すると、起動スクリプトが実行されずに、動作モードはセキュリティーモードのままになります。この状態でシステムを再起動すると、Security Officer レベルのユーザーが存在しないことになるため、多くのコマンドが実行できなくなります。このような状態になった場合は、「DISABLE SYSTEM SECURITY_MODE」コマンドを実行するしかありません。

ノーマルモードへ戻る

セキュリティーモードからノーマルモードに戻るには、次のコマンドを入力します。このコマンドを実行すると、「**enabled.sec**」が削除されます。また、ノーマルモードになった時点で、セキュリティーモードでのみ保存可能なファイル（暗号鍵ファイルなど）は自動的に削除されます。

```
Manager > DISABLE SYSTEM SECURITY_MODE ↵

Warning: This command will disable security mode and
    delete all security files.
Are you sure you wish to proceed?(y/n)  y

Info (1034003): Operation successful.
```

注意

このコマンドをご使用になる場合は、充分にご注意ください。削除された機密ファイルは復活できません。

6 テキストエディター

本章では、内蔵のテキストエディターの使い方について説明します。テキストエディターにより、例えば既存の設定ファイルを開き、編集を施して、保存することができます。

本書「9.2 ファイル名」(p.62)

6.1 Edit の実行

エディターの起動は、「EDIT」に続けて、ファイル名を指定します。拡張子は、cfg、scp、txt が指定可能です。指定したファイルが存在しない場合は、内容が空のファイルが作成されます。例えば、既存のファイル ROUTER.CFG を指定して、下記のコマンドを入力すると、

```
Manager > EDIT ROUTER.CFG ↲
```

次のようなエディター画面が表示されます。[*1]

```
#
# SYSTEM configuration
#

#
# SERVICE configuration
#

#
# LOAD configuration
#

#
# USER configuration
#
set user=manager pass=3af116ce503efb5dbf7a00c6cad64467bf priv=manager lo=yes
set user=manager desc="Manager Account" telnet=yes

#
# TTY configuration
#
Ctrl+K+H = Help | File = ROUTER.CFG | Insert | | 1:1
```

画面の最下行は、ステータス行です。左側から下記の項目を表示しています。

- ヘルプを表示するキー（Ctrl+K+H = Help）
- ファイル名（File = ROUTER.CFG）
- Insert（挿入モード）または Overstrike（上書きモード）
- 内容が変更されているか否か（変更ありは Modified と表示）
- カーソル位置（行番号：列番号）

カーソル移動キー（←↑↓→）を操作してみてください。カーソルが正しく移動しない場合は、通信ソフトウェアのエミュレーションを VT100 に設定してください。

本書「A.3 ハイパーターミナルの設定」(p.134)
本書「A.2 Microsoft Telnet の設定」(p.133)

「↓」キーを押し続け、カーソルが最下行まで移動すると、画面がスクロールします。ハイパーターミナルをご使用の場合、スクロールしたときに、長い行の右側が正しく表示されませんが、「Ctrl」キーを押しながら「W」キーを押すと、画面が再描画されます。

シャープ「#」で始まる行は、コメント行です。この行は、設定として解釈されません。カーソルをコメント行に移動して、「BackSpace」キーを押してみてください。文字を消去できない場合は、通信ソフトウェアの「BackSpace」キーのコードを「Delete」に設定してください。また、「Delete」キーでも文字を消去することができます。

内容を変更せずにエディターを終了する場合、「Ctrl」キーを押しながら「C」キーを押します。変更内容を破棄するか否かを問われますので、「Y」キー（はい）を押してください。「N」キーを押すと、エディター画面に戻ります。

```
Lose changes ( y/n ) ? Y
```

内容を保存する場合は、「Ctrl」キーを押しながら「K」キーを押し、続けて「Ctrl」キーを押したまま「X」キーを押します。保存するか否かを問われますので、「Y」キーを押してください。「N」キーを押すと、内容を保存せずにエディターが終了します。

```
Save file ( y/n ) ? Y
```

*1 入力されたコマンドは、本製品のルールにしたがった書式に変換されるため、実際に入力したコマンドと、「CREATE CONFIG=*filename*.CFG」で保存されたファイルのコマンドの見かけは異なったものとなります。しかしながら、保存されている設定情報は同じです。類似の概念として、「コマンドの分割入力」(p.36) をご覧ください。

6.2 キー操作

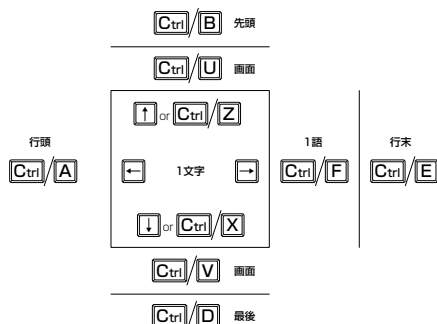



図6.2.1 カーソル移動キー

キー操作は、以下の通りです。「Ctrl/△」は「Ctrl」キーを押しながら「△」キーを押す操作を意味します。

「Ctrl/△, Ctrl/○」は、「Ctrl」キーを押しながら「△」キーを押し、続けて「Ctrl」キーを押しながら「○」を押す操作を意味します。

表 6.2.1：カーソル移動

キー	機能
↑[a] または Ctrl/Z	1 行上に、移動する。
↓または Ctrl/X	1 行下に、移動する。
→	1 桁右に、移動する。
←	1 桁左に、移動する。
Ctrl/B	ファイルの先頭に、移動する。
Ctrl/D[b]	ファイルの最後に、移動する。
Ctrl/A	行頭に、移動する。
Ctrl/E	行末に、移動する。
Ctrl/U	1 画面前に、移動する（スクロールダウン）。
Ctrl/V	1 画面後に、移動する（スクロールアップ）。
Ctrl/F	1 ワード右に移動する。

a. ハイパーターミナルをご使用の場合、カーソル移動キー↑↓→←は使用できません。
b. Ctrl/D を入力すると Telnet セッションが切断されることがありますのでご注意ください。

表 6.2.2：モードの切り替え

キー	機能
Ctrl/O	上書きモード
Ctrl/I	挿入モード

表 6.2.3：消去

キー	機能
Ctrl/T	カーソル右の 1 ワードを消去する。
Ctrl/Y	行全体を消去する。
BackSpace、Delete[a]	カーソル右の 1 文字を消去する。

a. ハイパーターミナルをご使用の場合、「ファイル」→「プロパティ」→「設定」→「Backspace キーの送信方法」を「Delete」に設定してください。

表 6.2.4：ブロック操作

キー	機能
Ctrl/K, Ctrl/B	ブロックマークを開始する。
Ctrl/K, Ctrl/C	ブロックでコピーする。
Ctrl/K, Ctrl/D	ブロックマークを終了する。
Ctrl/K, Ctrl/P	ブロックでペースト（貼りつけ）する。
Ctrl/K, Ctrl/U	ブロックでカットする。
Ctrl/K, Ctrl/Y	ブロックで消去する。
Ctrl/F	1 ワード右に移動する。

表 6.2.5：検索

キー	機能
Ctrl/K, Ctrl/F	文字列を検索する。
Ctrl/L	検索を再実行する。

表 6.2.6：終了・保存

キー	機能
Ctrl/K, Ctrl/X	上書き保存し、エディターを終了する。
Ctrl/C	変更を破棄するか問い合わせを表示してエディターを終了する。

表 6.2.7：その他

キー	機能
Ctrl/W	画面をリフレッシュ（再表示）する。
Ctrl/K, Ctrl/O	別のファイルを開く。
Ctrl/K, Ctrl/H	エディターのオンラインヘルプを表示する。

本製品は、Telnet デーモン（サーバー）およびクライアントの機能を内蔵しています。この章では、Telnet を使用するための設定や、操作について説明します。

7.1 本製品に Telnet でログインする

本製品は、Telnet デーモンを内蔵しており、他の Telnet クライアントからネットワーク経由でログインすることができます。

本書「A.2 Microsoft Telnet の設定」(p.133)

LAN 側Ethernet インターフェース経由でログインするためには、本製品に次のような設定が施されている必要があります。

```
Manager > ENABLE IP ↵
Manager > ADD IP INT=vlan1 IP=192.168.1.1 ↵
```

1 通信機能を利用できるコンピューターを使用し、本製品に対して Telnet を実行します。下記では、あらかじめ本製品の物理ポートに IP アドレス「192.168.1.1」が割り当てられていると仮定しています。実際には、お客様の環境におけるものをご使用ください。

```
TELNET 192.168.1.1 ↵
```

2 本製品に接続すると、ログインプロンプトが表示されますので、ユーザー名、パスワードを入力してください。下記では、デフォルトのManager レベルのユーザー名、パスワード（入力は表示されません）を仮定しています。ログインに成功すると、コマンドプロンプトが表示されます。

```
TELNET session now in ESTABLISHED state

 login: manager ↵
Password: friend ↵


Manager >
```

セキュリティーモードでは、Security Officer レベルのユーザーは Telnet でログインできなくなります（他のレベルなら可）。Security Officer レベルでログインするためには、Remote Security Officer の設定が必要です。

本書「 セキュリティーモードへの移行」(p.52)

7.2 ブリッジングにおける Telnet

リモートブリッジとして動作するように設定されている場合（IP がブリッジングされている）においても、Ethernet または WAN インターフェース経由のIP アクセスが可能です。これにより Ethernet 側や WAN 回線を経由して、Telnet クライアントによる本製品へのログイン、または本製品を Telnet クライアントとして動作させることができます。下記にローカルブリッジにおける設定例を示します（IP の機能モジュールを有効化し、Ethernet インターフェースにIP アドレスを割り付けています)。

```
ENABLE BRIDGE ↵
ADD BRIDGE PROTOCOL="ALL ETHERNET II"
   TYPE=ALLETHII PRIO=1 ↵
ADD BRIDGE PROTOCOL="IP" TYPE=IP PRIO=1 ↵
ADD BRIDGE PROTOCOL="ARP" TYPE=ARP PRIO=1 ↵
ADD BRID PO=1 INT=vlan1 ↵
ADD BRID PO=2 INT=eth0 ↵
ENABLE IP ↵
ADD IP INT=eth0 IP=192.168.5.1 ↵
```

図 7.2.1 ブリッジングにおける IP アクセスのための設定

Telnet クライアントから 192.168.5.1 にアクセスすると、

```
TELNET 192.168.5.1 ↵
```

プロンプト「login:」が表示されます。

```
TELNET session now in ESTABLISHED state

login:
```

7.3 TELNET コマンドの実行

本製品は、Telnet クライアントの機能を内蔵しているため、本製品から他の機器に対して Telnet を実行することができます。[*1]

本製品に Manager レベルでログインし、「TELNET」コマンドを実行します。以下では、接続先の IP アドレスを「192.168.10.1」と仮定しています。実際には、お客様の環境におけるものをご使用ください。

```
Manager > TELNET 192.168.10.1 ↵
```

IP アドレスのホスト名を設定する

IP アドレスの代わりに分かりやすいホスト名を設定することができます。例えば、上記の例の IP アドレスのホスト名が「pearl」であると仮定すると、次のコマンドを入力します。

```
Manager > ADD IP HOST=pearl IP=192.168.10.1 ↵
```

ホスト名を使用して、Telnet を実行することができます。

```
Manager > TELNET pearl ↵
```

DNS サーバーを参照するように設定する

ホスト名から IP アドレスを得るために、DNS サーバーを参照するように設定することができます。DNS サーバーの IP アドレスが「192.168.10.200」であると仮定すると、次のコマンドを入力します。

```
Manager > ADD IP PRIMARY=192.168.10.200 ↵
```

ホスト名を使用して、Telnet を実行することができます。

```
Manager > TELNET spankfire.deilla.co.jp ↵
```

ヒント

*1 コンピューターでマルチウインドウの Telnet が使える場合は、本製品にログインして「TELNET」コマンドを実行するよりは、コンピューターで複数の Telnet セッションを実行する方が便利です。

8.1 Ping

「PING」コマンドによって、指定した相手との通信が可能かどうかを確認することができます。PING は、指定した相手にエコーを要求するパケットを送信し、相手からの応答を表示します。

IP における例を下記に示します。PING に続けて IP アドレスを指定します。デフォルトの回数は5回です。

```
Manager > ping 192.168.1.100 ↵

Echo reply 1 from 192.168.1.100 time delay 1 ms

Echo reply 2 from 192.168.1.100 time delay 1 ms

Echo reply 3 from 192.168.1.100 time delay 1 ms

Echo reply 4 from 192.168.1.100 time delay 1 ms

Echo reply 5 from 192.168.1.100 time delay 1 ms
```

相手のみを指定して PING を打つと、発信元の IP アドレスとして送出インターフェースの IP アドレスが付加されます。これを防ぐためには明示的に発信元の IP を指定します。また、この明示的な IP はルーター内部に設定済みのIP でなければいけません。

```
Manager > ping 192.168.1.100
    sipa=192.168.1.1 ↵
```

PING に対する応答がある場合、「Echo reply 1 from xxxxxx time delay xx ms」のように表示されます。PING に対する応答がない場合、「Request 1 timed-out: No reply from xxxxxx」のように表示されます。「No route to specified destination」のように表示される場合、経路情報が未設定か、設定内容に誤りがあります。

「SET PING」コマンドにより、PING のオプションを設定することができます。「SHOW PING」コマンドにより、PING の設定情報を表示します。「STOP PING」コマンドにより、実行中の PING を中止します(PING はバックグラウンドで実行されます。PING の結果が次々に表示されている状態でも、コマンドの入力は可能です)。

8.2 Trace

「TRACE」コマンドによって、指定した相手までの実際の経路を表示することができます。

```
Manager > trace 192.168.80.121 ↵

Trace from 192.168.28.128 to 192.168.80.121, 1-30 hops
 1. 192.168.48.32         0     13     20 (ms)
 2. 192.168.83.33        20     20     20 (ms)
 3. 192.168.80.121        ?     40      ? (ms)
***
Target reached
```

「SET TRACE」コマンドにより、TRACE のオプションを設定することができます。「SHOW TRACE」コマンドにより、TRACE の設定情報を表示します。「STOP TRACE」コマンドにより、実行中の TRACE を中止します(TRACE はバックグラウンドで実行されます。TRACE の結果が次々に表示されている状態でも、コマンドの入力は可能です)。

9.1 ファイルシステム

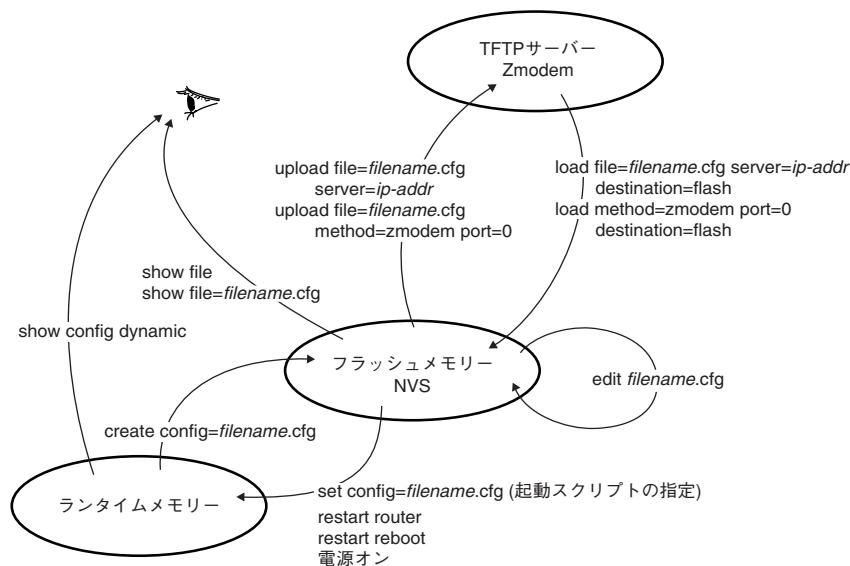



図9.1.1 設定ファイルに関するコマンド

本製品は、システム再起動後もデータが保持される 2 次記憶装置として、次の2つを内蔵しています。

- フラッシュメモリー（32MB）：ファームウェアファイル、パッチファイル、設定スクリプトなどを保存
- NVS[*1]（512KB）：モジュールのコンフィグレーションテーブルや、パッチファイル、スクリプトファイルなどを保存

これらのメモリーは、コンピューターにおけるはハードディスクのように振る舞います。電源をオンにすると、これらのメモリーからファームウェアファイルをロードし、起動スクリプトファイル（.CFG）が指定されていれば、それもロードして実行します。

「SHOW FILE」コマンドによって、フラッシュメモリー、NVS に保存されているファイルの一覧を表示することができます。下記に例を示します(実際のファイル名は、お客様の環境、保存されているファームウェアなどのバージョンによって異なります)。

```
Manager > SHOW FILE ↵

Filename          Device   Size       Created          Locks
------------------------------------------------------------
55275b03.rez       flash  3553292  24-MAR-2006 14:37:22  0
example_isp.cfg    flash  2840     25-MAR-2006 11:29:23  0
feature.lic        flash  39       24-MAR-2006 14:55:15  0
help.hlp           flash  106718   24-MAR-2006 14:45:09  0
longname.lfn       flash  89       25-MAR-2006 19:38:58  0
prefer.ins         flash  64       24-MAR-2006 14:41:16  0
random.rnd         flash  3904     02-MAR-2006 11:09:54  0
release.lic        flash  256      15-MAR-2006 15:37:22  0
test01.cfg         flash  2840     25-MAR-2006 11:29:23  0
ud.cfg             flash  5428     18-MAR-2006 16:57:44  0
------------------------------------------------------------
```

ヒント

*1 Non-Volatile Storage、バッテリーバックアップされたCMOS メモリー

「SHOW FLASH」コマンドによって、フラッシュメモリーの状態を表示することができます。

```
Manager > SHOW FLASH ↵

FFS info:
global operation ...... none
flash autowrite ....... disabled
compaction count ...... 16
est compaction time ... 564 seconds
files ................ 24537096 bytes  (28 files)
garbage ...............      432 bytes
free .................  7837256 bytes
required free block ...   131072 bytes
total ................ 32505856 bytes

diagnostic counters:
event      successes        failures
-------------------------------------
get                0               0
open               0               0
read              15               0
close              8               0
complete           0               0
write              0               0
create             0               0
put                0               0
delete             0               0
check              1               0
erase              0               0
compact            0               0
verify             0               0
-------------------------------------
```

フラッシュメモリーのコンパクション

「ACTIVATE FLASH COMPACTION」コマンドにより、フラッシュメモリーのコンパクション（ガベッジの除去）を行うことができます。

通常の運用であれば、このコマンドを使用する必要はほとんどありませんが、フラッシュメモリーは空いているはずなのに、ファイルがロードできないといった状況では、このコマンドを実行してみます。

```
Manager > ACTIVATE FLASH COMPACTION ↵

Info (131260): Flash compacting...
DO NOT restart the router until compaction is completed.
```

コンパクションは、バックグラウンドで実行されます。コンパクションが完了して、次のメッセージが表示されるまで、<u>絶対に本製品の電源をオフにしたり、「RESTART」コマンドを実行しないでください</u>（状況によっては、1～5分かかることがあります。）。

```
Manager >
Info (131261): Flash compaction successfully completed.
```

コンパクション実行中に、絶対に本製品の電源をオフにしたり、「RESTART」コマンドを実行しないでください。リスタートや電源オフを行うと、ファイルシステムが破壊されます。

ファームウェアのバージョンアップなどで使用するセットアップツールは、ファームウェアなどの大きなファイルを削除したとき、自動的にこのコンパクションが実行されます。

9.2 ファイル名

ファイル名は、次の形式で表されます。*filename* と *ext* はピリオドで結びます。*device* の後にはコロンを入れます。ディレクトリー（フォルダー）の概念はありません。

```
[device:]filename.ext
```

device
　デバイス名。「flash」「nvs」のいずれか。大文字・小文字の区別はありません。省略すると「flash」を指定したことになります。

filename
　ファイル名（ベース名）。文字数は 1 ～ 16 文字。半角英数字とハイフン（-）が使えます。大文字・小文字の区別はありませんが、表示には大文字・小文字の区別が反映されます。

ext
　拡張子。ファイル名には必ず拡張子をつけなければなりません。表 9.2.1 の拡張子が使用可能です。大文字・小文字の区別はありませんが、表示には大文字・小文字の区別が反映されます。

「UserDoc.CfG」のように大文字・小文字混ざりのファイルを作成することが可能です。しかしながら、大文字・小文字の属性は無視されるため、「UserDoc.CfG」が作成されていれば「userdoc.cfg」は作成できませんし、「userdoc.cfg」を指定すると「UserDoc.CfG」が対象となります。

表 9.2.1 に本製品が使用する主な拡張子を示します。

表9.2.1 主な拡張子

拡張子	ファイルタイプ / 機能
REZ	本製品が起動するとき、ロードされるファームウェアの圧縮形式のファイル
PAZ	ファームウェアに対するパッチの圧縮形式のファイル。ソフトウェアのバージョンによっては、インストールされていない場合もあります
CFG	本製品の設定スクリプトファイル[a]。「SCP」との間に明確な区別はありませんが、慣例として設定内容を保存するスクリプトには「CFG」を使います
SCP	実行スクリプトファイル。「CFG」との間に明確な区別はありませんが、慣例としてトリガースクリプトやバッチファイル的なスクリプトには「SCP」を使います
HLP	オンラインヘルプのファイル
LIC	ライセンスファイル。ファームウェア（リリース）や追加機能（フィーチャー）のライセンス情報を格納しているファイルです。絶対に削除しないでください
INS	起動時に読み込むファームウェアや設定ファイルの情報を格納しているファイル
DHC	DHCP サーバーの設定情報ファイル
TXT	プレーンテキストファイル

a. CFG、SCP ファイルの内容において、「#」で始まる行は、コメントと見なされ無視されます。

特に、EDIT コマンドは、CFG、SCP、TXT の拡張子を持つファイルを指定することができます。

本書「6 テキストエディター」（p.55）

表9.2.2 特別な役割を持つファイル

ファイル名	役割
boot.cfg	デフォルトの起動スクリプトファイル。 「SET CONFIG」コマンドで起動スクリプトが設定されていない（none）場合、本ファイルが存在していれば起動時に自動実行されます。 起動スクリプトが設定されている場合は、設定されているファイルが実行されます
config.ins	起動スクリプトファイルの情報を保存しているファイル。「SET CONFIG=*filename*.CFG」を実行すると作成（上書き）されます。「SET CONFIG=NONE」を実行すると削除されます
prefer.ins	起動時にロードするファームウェア、パッチファイルの情報を保存しています
enabled.sec	セキュリティーモードへ移行したときに自動的に作成されるファイル。システムに対し、起動時にセキュリティーモードへ移行すべきことを示すファイルです
random.rnd	IPsec などの暗号化のためのテーブルとして自動的に作成されるファイル。内部処理のために使われるもので、ユーザーが意識する必要はありません
release.lic	リリースライセンスファイル。ファームウェア（リリース）のライセンス情報を持つファイルです。削除しないでください
feature.lic	フィーチャーライセンスファイル。追加機能（フィーチャー）のライセンス情報を持つファイルです。削除しないでください
longname.lfn	短いファイル名（8.3 形式）と長いファイル名（16.3 形式）の対応を保持しています。ファイル名（ベース名）部分が 8 文字を超えるファイルを作成すると自動的に作成され、以後自動的に更新されます。削除しないでください

9.3 ワイルドカード

ファイルを操作する次のコマンドは、ワイルドカード（*）を使って複数のファイルを一度に指定できます。

- DELETE FILE コマンド
- SHOW FILE コマンド

ワイルドカード（*）は「任意の文字列」を示すもので、例えば下記はすべての設定スクリプトファイルを表示します。

```
Manager > SHOW FILE=*.cfg ↵

Filename            Device        Size      Created                Locks
------------------------------------------------------------------------
52catv.cfg          flash         2199      08-May-2002 21:48:14    0
53perso.cfg         flash         3223      08-May-2002 22:00:07    0
55mulho.cfg         flash         3149      08-May-2002 22:36:19    0
example_isp.cfg     flash         2840      25-Mar-2005 11:29:23    0
telnet.cfg          flash         2324      26-Apr-2002 16:11:25    0
tokyo.cfg           flash         4511      09-May-2002 01:30:02    0
tokyo.scp           flash         2430      11-May-2002 21:45:06    0
x-y.cfg             flash         2276      11-May-2002 20:44:19    0
y-z.cfg             flash         2359      11-May-2002 21:46:33    0
------------------------------------------------------------------------
```

filename 部分では「*string**」のような使い方ができます。ext 部分では、単独で適用します。例えば、下記は「t」で始まるファイルを表示します。ただし、*filename* 部分に対して「**string*」「*str*ing*」のような使い方はできません。

```
Manager > SHOW FILE=t*.* ↵

Filename            Device        Size      Created                Locks
------------------------------------------------------------------------
telnet.cfg          flash         2324      26-Apr-2002 16:11:25    0
tokyo.cfg           flash         4511      09-May-2002 01:30:02    0
tokyo.scp           flash         2430      11-May-2002 21:45:06    0
------------------------------------------------------------------------
```

下記は、no で始まるフラッシュメモリーの scp ファイルのすべてを削除します。

```
Manager > DELETE FILE=no*.scp ↵
```

下記は、no で始まるフラッシュメモリー、NVS 両方の scp ファイルのすべてを削除します。

```
Manager > DELETE FILE=*:no*.scp ↵
```

注意

削除してしまったファイルの復旧はできません。「DELETE FILE=*.*」を使用してファイルを削除するとすべてのファイルが削除され、本体が起動できなくなります。ワイルドカードを使用したファイルの削除は、充分にご注意ください。

10 設定ファイルのバックアップとリストア

本製品は、フラッシュメモリー、NVS に保存されている設定ファイルなど[*1] のバックアップやリストア（復元）を行うことができます。

TFTPサーバー
Zmodem
192.168.1.100
ダウンロード
(LOAD)
リストア
アップロード
(UPLOAD)
バックアップ
AR570S
192.168.1.1

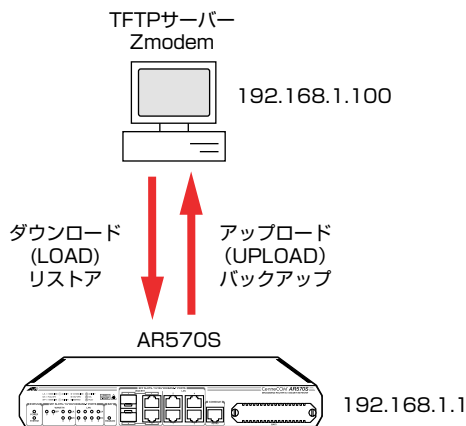



図 10.0.1 アップ / ダウンロード

本章では、TFTP、Zmodem によるバックアップとリストアについて説明します。

10.1 TFTP

本製品は、TFTP クライアントの機能を内蔵しており、TFTP サーバーから本製品のフラッシュメモリー、NVS へのダウンロード、または本製品のフラッシュメモリー、NVS からTFTP サーバーへのアップロードが可能です（フラッシュメモリーがデフォルトの操作対象となります[*2]）。

本書「9 ファイルシステム」（p.61）

TFTP 機能を利用するためには、次のような設定が本製品に施されている必要があります。

```
Manager > ENABLE IP ↵
Manager > ADD IP INT=vlan1 IP=192.168.1.1 ↵
```

以下の説明では、LAN 側インターフェース VLAN1（192.168.1.1）に、TFTP サーバー（192.168.1.100）が直接接続されていると仮定します。

*1 ファームウェア、パッチファイルなどは、アップロードできません。

*2 「LOAD」コマンドの「DESTINATION」パラメーターで指定できます。また、「SET LOADER」コマンドでデフォルトが変更できます。

アップ / ダウンロードは、ノーマルモードの場合はManager レベル、セキュリティーモードの場合はSecurity Officer レベルの権限が必要です。

ダウンロード

ダウンロードは、「LOAD」コマンドを使用します。次に、入力例を示します。ファイル名として「test01.cfg」を仮定しています。

```
Manager> LOAD FILE=test01.cfg
    SERVER=192.168.1.100
    DESTINATION=FLASH ↵

Manager >
Info (1048270): File transfer successfully completed.
```

きちんとダウンロードできたかは、「SHOW FILE」コマンドで確認できます。

TFTP サーバーによっては（UNIX 系OS の tftpd など）、ファイルをダウンロードする際に、ファイル名の大文字・小文字を区別しますのでご注意ください。フラッシュメモリー上では大文字・小文字の区別はありませんが、表示には大文字・小文字の区別が反映されます。

TFTP では、ダウンロードするファイルと同名のファイルが、フラッシュメモリー、NVS 上に存在する場合、ダウンロードできません。「DELETE FILE」コマンドでフラッシュメモリー上のファイルを削除してからダウンロードしてください。

アップロード

アップロードは、「UPLOAD」コマンドを使用します。次に、入力例を示します。ファイル名は、大文字・小文字を識別します。

```
Manager> UPLOAD FILE=test01.cfg
    SERVER=192.168.1.100 ↵

Manager >
Info (1048270): File transfer successfully completed.
```

TFTP サーバーによっては（UNIX 系OS の tftpd など）、ファイルをアップロードする際に、TFTP サーバーでファイルのクリエイト（作成）ができないために、アップロードが失敗することがあります。そのような場合は、TFTP サーバーのディレクトリーに、あらかじめアップロードされるファイルと同じ名前のファイルを作成し、書き込める権限をあたえておいてください（UNIX 系 OS では、大文字・小文字を区別します）。

10.2 Zmodem

本製品は、Zmodem プロトコルを内蔵しており、コンソールポートに接続されているコンソールターミナルから本製品のフラッシュメモリー、NVS へのファイルのダウンロード、本製品のフラッシュメモリー、NVS からコンソールターミナルへのファイルのアップロードが可能です（フラッシュメモリーがデフォルトの操作対象となります[*3]）。

ここでは、通信ソフトウェアとして Windows 2000 のハイパーターミナルを使用する場合を説明します。

本書「A.3 ハイパーターミナルの設定」（p.134）
本書「9 ファイルシステム」（p.61）

ダウンロード

1 ハイパーターミナルを起動し、Manager レベルでログインしてください（セキュリティーモードの場合は、Security Officer レベルでログインしてください）。

2 ダウンロードは、「LOAD」コマンドを使用します。次に、入力例を示します。Zmodem によるダウンロードでは、フラッシュメモリー、NVS 上に同名のファイルが存在する場合、上書きされずにコマンドはすぐに終了しますのでご注意ください。

```
Manager> LOAD METHOD=ZMODEM ASYN=0
    DESTINATION=FLASH ↵
```

3 画面に「Router ready to begin ZMODEM file transfers ...」と表示されたら、ハイパーターミナルのメニューバーから「転送」→「ファイルの送信」を選択し、ファイルを指定します。

4 指定したファイルを再確認し、良ければ「送信」ボタンをクリックします。

5 画面に「Zmodem, session over.」と表示されたらダウンロードは完了です。

6 「SHOW FILE」コマンドで本製品にきちんとダウンロードできたことを確認してください。

アップロード

1 ハイパーターミナルを起動し、Manager モードでログインしてください（セキュリティーモードの場合は、Security Officer レベルでログインしてください）。

2 アップロードは、「UPLOAD」コマンドを使用します。次に、入力例を示します。

```
Manager> UPLOAD FILE=TOOS.cfg METHOD=ZMODEM
    ASYN=0 ↵
```

3 ハイパーターミナルが自動的にファイル受信を開始します。

4 「File transfer successfully completed.」と表示されたら、アップロードは完了です。

*3「LOAD」コマンドの「DESTINATION」パラメーターで指定できます。また、「SET LOADER」コマンドでデフォルトが変更できます。

弊社は、改良のために、予告なく本製品のソフトウェアのバージョンアップやパッチレベルアップを行うことがあります。この章では、最新ファームウェアの入手方法や、バージョン番号について説明します。

11.1 必要なもの

本製品のバージョンアップには、次のものが必要です。

- 最新ファームウェアのダウンロードモジュール
  ファームウェア、ヘルプファイルなど、必要なファイルをまとめた自己解凍の圧縮ファイルです。

- リリースノート
  機能拡張、バグフィクス内容について説明した文書です。
  重要な情報が記載されていますので、必ずご覧ください。

- ファームウェアインストーラー
  ファームウェアなどのファイルを、本製品にダウンロードするツールです。

- バージョンアップ手順書
  バージョンアップの仕方、注意点が記載されています。

- Windows XP/2000/Me/98、Windows NT がインストールされたコンピューター
  ファームウェアインストーラーを実行します。

ダウンロードモジュール、リリースノート、ファームウェアインストーラー、バージョンアップ手順書、弊社 Web ページからダウンロードすることができます。

```
http://www.allied-telesis.co.jp/
```

11.2 ファイルのバージョン表記

ファームウェアファイル

ファームウェアのバージョンは、「*X.Y.Z-MM*」のような書式で表示されます。*1 *2
(例)「2.7.5-03」

ファームウェアのファイル名は、「55*XYZ-MM*.REZ」のような書式で表示されます。
(例)「55275-03.REZ」

参照 本書「9 ファイルシステム」(p.61)

ダウンロードモジュール

ダウンロードモジュールのファイル名は、「ar55*XYZMM*.exe」のような書式で表示されます。
(例)「ar5527503.exe」

*1 リリースによっては、ファームウェアバージョンの「*X.Y.Z*」の後に「.A」「.B」などのサフィックスがつく場合があります。

*2 製品底面などに貼付されているファームウェアバージョンラベルは「V.*X.Y.Z-MM* PL *A*」のような書式を持ちますが、通常「PL 0」となります。

本製品の使用中になんらかのトラブルが発生したときの対応方法について説明いたします。

12.1 トラブルへの対処法

LEDの観察

本製品前面のLEDの状態を観察してください。LEDの状態は問題解決のため役立ちますので、問い合わせの前にLEDの状態（点灯、点滅、消灯など）を、ご確認していただきますようお願いいたします。LEDの状態については、下記に説明があります。

本書「1.3 各部の名称と働き」（p.18）

自己診断テストの結果の確認

本製品は自己診断機能（セルフテスト）を備えています。異常発生時には、起動メッセージにエラー内容が表示されます。セルフテストは、次のような場合に実行されます。

- 電源を入れたとき
- RESTART REBOOTコマンドで再起動したとき
- 致命的なエラーによって自動的に再起動したとき

正常な起動時には次のようなメッセージが表示されます。

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 65536k bytes found.
INFO: Self tests complete.
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download successful.

INFO: Initialising Flash File System.


INFO: IGMP packet trapping is active for IGMP snooping,
    L3FILT is activated
INFO: Executing configuration script <flash:boot.cfg>
INFO: Router startup complete

 login:
```

起動メッセージは、下記の4つに分類されて表示されます。

- INFO：起動プロセスが表示されます
- PASS：テストが問題なく終了したことを意味し、結果が表示されます
- ERROR：テストでエラーが発生したことを意味し、エラー内容が表示されますが起動プロセスは続行されます
- FAIL：テストで致命的なエラーが発生したことを意味し、起動プロセスは中断されます

本製品のログを見る

本製品が生成するログを見ることにより、原因を究明できることがあります。ログは、「SHOW LOG」コマンドで表示できます。

```
 login: manager ↲
Password: ________ ↲

Manager > SHOW LOG ↲

Date/Time   S Mod  Type  SType Message
-------------------------------------------------------------------------------
26 14:18:02 4 ENCO ENCO  PAC   M18X Security Engine Found.
26 14:18:02 4 ENCO ENCO  PAC   M18X Security Engine Initialised.
26 14:18:02 3 LOG              IGMP packet trapping is active for IGMP
                               snooping, L3FILT is activated
26 14:18:02 4 ENCO ENCO  STAC  STAC SW Initialised
26 14:18:02 7 SYS  REST  NORM  Router startup, ver 2.7.5.B-03, 04-MAR-2006, Clock
                               Log: 14:17:13 on 26-MAR-2006
26 14:18:02 6 PRI  PINT  WARN  pri(0): interface reset
26 14:18:04 6 PRI  PINT  DOWN  pri(0): Interface is no longer receiving
                               incoming signal
26 14:18:16 3 DHCP DHCP  00001 IP address 192.168.1.100 bound to
                               00-00-f4-95-9c-96
26 14:18:31 3 DHCP DHCP  00001 IP address 192.168.1.101 bound to
                               00-90-99-7e-b3-bb
26 14:18:51 3 USER USER  LON   manager login on port0
26 14:18:55 3 CH   MSG   WARN  No patches found
26 14:20:39 3 CH   MSG   WARN  No patches found
26 15:18:16 3 DHCP DHCP  00001 IP address 192.168.1.100 bound to
--More--  (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

図 12.1.1 ログの表示例

12.2 トラブル例

コンソールターミナルに文字が入力できない

- コンソールケーブルは正しく接続されているか
- 通信ソフトウェアを 2 つ以上同時に起動していないか。複数の通信ソフトウェアを同時に起動するとCOMポートで競合が発生し、通信できない、不安定になるなどの障害が発生する
- 通信ソフトウェアの設定内容は正しいか。特に、コンソールケーブルを接続している COM ポート名と、通信ソフトウェアで設定している COM ポート名は一致しているか

本書「A.3 ハイパーターミナルの設定」(p.134)

- 通信ソフトウェアを一旦終了し、再度起動してみる
- コンピューターの再起動からやってみる

コンソールターミナルで文字化けする

- 通信ソフトウェアの通信速度は9,600bps に設定してあるか。本製品のご購入時の設定は9,600bps
- 通信ソフトウェアのエンコードをシフト JIS（SJIS）に設定する。HELP コマンドは、シフト JIS で日本語を表示する

本書「A.3 ハイパーターミナルの設定」(p.134)

- 入力モードは、英数半角モードになっているか。全角文字や半角カナは入力できない。Windows では、「Alt」キーを押しながら「半角 / 全角」キーを押して切り替える

EDIT のトラブル

「BackSpace」キーで文字が消せない

- 通信ソフトウェアの「BackSpace」キーのコードをDeleteにする
- 「Delete」キーを使う

本書「A.3 ハイパーターミナルの設定」(p.134)
本書「6 テキストエディター」(p.55)

カーソルキーが利かない

- 通信ソフトウェアのエミュレーションをVT100 にする

ハイパーターミナルで画面右の文字がスクロールしない

- 「Ctrl」キーを押しながら「W」キーを押して画面を再描画する
- Tera Term などの通信ソフトウェアを使用する

再起動したらプロバイダーに接続しない

- PPPoE による接続において、正しい手順による再起動、本製品の電源スイッチオフを行わなかった場合、しばらくの間プロバイダーとの接続ができなくなることがあります。数分〜十数分待った後、接続状態を確認してみてください。

本書「再起動時のご注意」(p.32)

POWER LED が点灯しない

POWER LED の消灯は、本製品に電源が供給されていないことを示しています。以下の点を確認してください。

- 電源スイッチは、オンになっているか
- 電源ケーブルは、本製品の電源コネクターに正しく接続されているか
- ACプラグは、電源コンセントに正しく接続されているか
- 電源コンセントには、電源が供給されているか

SYSTEM LED が点灯する

1 本製品の電源をオフにし、しばらく待ってオンにします。

2 SYSTEM LED が橙に点灯し続けていたら、本製品に異常が発生していることを示しています。

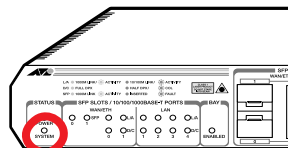



図 12.2.1 前面図

起動時の一時的な点灯は、本製品の異常を示すものではありません。

LINK LED（L/A）が点灯しない

LINK LED の消灯は、該当の 10BASE-T/100BASE-TX/1000BASE-T ポートに接続されている機器との通信ができないことを示しています。以下の点を確認してください。

- UTP ポートと同じ番号の SFP スロットに、SFP モジュールが装着されていないか。UTP ポートと SFP スロットはコンボ（共

有）ポートとなっているため、SFP モジュールを装着すると、UTP ポートは無効となる

- 接続先機器の電源は、オンになっているか
- UTPケーブルは、本製品と接続先機器に接続されているか
- 本製品の該当のポートに接続されているUTP ケーブルを、本製品の他のポートに接続してみる。他のポートでも消灯のままなら、接続先機器側またはUTP ケーブルの問題
- UTP ケーブルを接続先機器の他のポートに接続してみる。他のポートでも消灯のままなら、本製品側または UTP ケーブルの問題
- 正常に接続できることが分かっている、他の UTP ケーブルに交換してみる
- 正しいUTP ケーブルを使用しているか。1000BASE-T の場合はエンハンスド・カテゴリ5、100BASE-TX の場合はカテゴリー5 以上、10BASE-T の場合はカテゴリー3 以上
- UTP ケーブル長は正しいか。ケーブル長は最大 100m

LINK LED（L/A）が点灯しているのに通信できない

- LAN 側ポートの場合、ポートが無効に設定されていないか。「SHOW SWITCH PORT」コマンドでポートステータス（Status）を確認する
- 接続先機器側のLINK LED は点灯しているか。LINK LED は、本製品と接続先機器の両方にあり、両方が点灯していなければならない
- 正しいUTP ケーブルを使用しているか。1000BASE-T の場合はエンハンスド・カテゴリ5、100BASE-TX の場合はカテゴリー5 以上、10BASE-T の場合はカテゴリー3 以上
- UTP ケーブル長は正しいか。ケーブル長は最大 100m

SFP LED が緑色に点灯しない

SFP LED が緑色に点灯していない場合は、該当の SFP スロットの SFP モジュールの光ポートに接続されている機器との通信ができないことを示しています。以下の点を確認してください。

- 光ファイバーケーブルは正しく接続されているか。本製品の TX は接続先機器のRX に、本製品の RX は接続先機器の TX に接続しなければならない。本製品側の TX と RX のファイバーの接続を入れ替えてみて、緑色に点灯すれば、接続の誤り

SFP LED が緑色に点灯しているのに通信できない

- 接続先機器側の SFP LED は点灯しているか。SFP LED は、本製品と接続先機器（接続先機器の LED 名称が SFP LED ではないことがあります）の両方にあり、両方が点灯していなければならない。一方のみの LED の点灯は、光ケーブルの断線や中継点の異常が考えられる

第２部　設定例編

ここでは、本製品がよく使われる環境をいくつかとりあげ、その設定方法について解説します。

13 構成例

ここまでの章で、運用・管理に関することがらや、ソフトウェア的な内部構造について説明しました。本章では、よく使われまた便利な構成を挙げて、設定の要点を説明しつつ、必要なコマンド入力を示します。さらに高度な設定に進むための、はじめの一歩としてお読みください。

本章の構成は、下記のようになっています。まず、インターネット接続について、4 例を説明します。

- 13.2 PPPoE による端末型インターネット接続（p.76）
- 13.3 PPPoE による LAN 型インターネット接続（アンナンバード）（p.80）
- 13.4 PPPoE による LAN 型インターネット接続（DMZ の設定）（p.84）
- 13.5 Ethernet による端末型インターネット接続（p.89）

次に、IPsec を利用してセキュリティーを確保しながらインターネット経由で、複数の拠点における LAN を相互接続する方法を説明します。

- 13.6 インターネット接続による 2 点間 IPsec VPN（p.93）
- 13.7 インターネット接続による 3 点間 IPsec VPN（p.104）

そして、PPPoE のマルチセッションを用い、インターネット接続と、NTT 東日本のフレッツ・グループアクセスや NTT 西日本のフレッツ・グループなどの CUG サービスを同時に利用する方法を説明します。

- 13.8 インターネットと CUG サービスの同時接続（端末型）（p.118）
- 13.9 インターネットと CUG サービスの同時接続（LAN 型）（p.122）

最後に、PPPoE の自動接続を行うための設定の詳細と、注意事項など、知っておいていただきたい情報をまとめてあります。実際に設定を始める前にご覧ください。

- 13.10 設定上の注意事項（p.128）
  - 「PPPoE セッションの手動による切断」（p.128）
  - 「PPPoE セッションの再接続」（p.128）
  - 「PPPoE におけるアンナンバード」（p.128）

13.1 設定をはじめる前に

コマンド入力における注意

下記にコマンドの入力例を示します。実際に入力する部分は、太文字で示します。「↵」は、リターンキーまたはエンターキーです（本書では、リターンキーと表記します）。

紙面の都合により、コマンドを折り返す場合は、2 行目以降を字下げします。実際のコマンド入力では、字下げされている行の前にスペースひとつを入れ、「↵」まで 1 行で入力してください。

（例）

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

コマンド入力の便宜のために

付属の CD-ROM に、この章で入力する全コマンドを収録したテキストファイル（¥SAMPLE¥570SAMP.TXT）があります。

このファイルをご使用のコンピューターにコピーし、あらかじめテキストエディターでお客様固有の部分を修正した後、テキストエディターからコンソールターミナルに、コマンドをコピー＆ペーストしてください。

一度に 1 行ずつコピー＆ペーストし、表示されるメッセージを確認しながら進めるのが安全です。一度に全部の行をコピー＆ペーストすると、バッファーがあふれたり、メッセージが確認できないために、正常にコマンドが実行されたことが分かりません。

TFTP や Zmodem を使用して、直接本製品にダウンロードすることも可能ですが、実際に 1 行ずつコマンドを入力してみることをお勧めします。

13.2 PPPoE による端末型インターネット接続

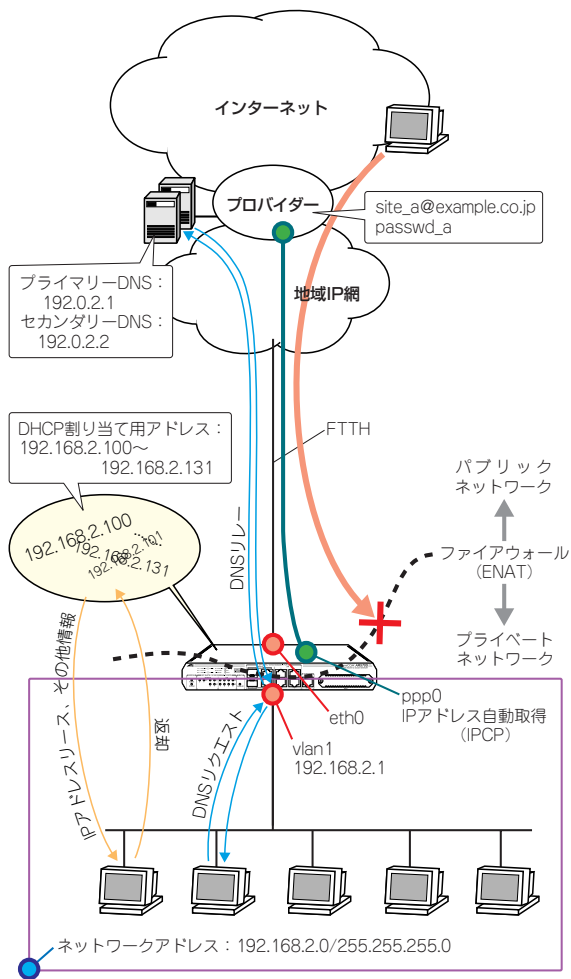



図 13.2.1 PPPoE による端末型の接続

PPPoE を使ってプロバイダーに接続します。PPPoE は、ADSL や FTTH などのいわゆる「ブロードバンド」系サービスで広く使用されているプロトコルです。この例は、接続するとき動的にアドレスを 1 つ割り当てられる端末型の基本設定です。

ダイナミック ENAT で 1 個のアドレスを共用し、ファイアウォールで外部からの不正アクセスを防止します。また、LAN 側クライアントの設定を簡単にするため、DNS リレーと DHCP サーバーも利用します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：1 個（動的割り当て）
- DNS サーバー：接続時に通知される

設定の方針

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。

- ファイアウォールのダイナミック ENAT 機能を使用して、LAN 側ネットワークのプライベート IP アドレスを、プロバイダーから与えられたグローバルIP アドレスに変換します。これにより、LAN に接続された複数のコンピューターからインターネットへの同時アクセスが可能になります。

- 本製品の IP アドレスは、下記のように設定します。

表 13.2.1 本製品の基本設定

WAN 側物理インターフェース	eth0
WAN 側（ppp0）IP アドレス	接続時にプロバイダーから取得する
LAN 側（vlan1）IP アドレス	192.168.2.1/24
DHCP サーバー機能	有効

- 本製品を DHCP サーバーとして動作させ、LAN に接続されたコンピューターに IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバーアドレスの情報を提供します。

表 13.2.2 本製品の DHCP サーバーの設定

DHCP ポリシー名	BASE
使用期限	7200（秒）
サブネットマスク	255.255.255.0
デフォルトルート	192.168.2.1
DNS サーバー	192.168.2.1
DHCP レンジ名	LAN
提供する IP アドレスの範囲	192.168.2.100 ～ 192.168.2.131（32 個）

- 本製品の DNS リレー機能をオンにして、LAN 側コンピューターからの DNS リクエストを、プロバイダーの DNS サーバーに転

送します。上記 DHCP サーバーの設定により、LAN 側コンピューターに対しては、DNS サーバーアドレスとして本製品自身の IP アドレスを教えます。

設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

●PPP の設定

3 WAN 側 Ethernet インターフェース（eth0）上にPPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

4 プロバイダーから通知されたPPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視し、自動的に PPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=site_a@example.co.jp
    PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

●IP、ルーティングの設定

5 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

6 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するように設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.
```

7 LAN 側（vlan1）インターフェースに IP アドレスを設定します。

```
Manager > ADD IP INT=vlan1 IP=192.168.2.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

8 WAN 側（ppp0）インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

9 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

●DNS リレーの設定

10 DNS リレー機能を有効にします。

```
Manager > ENABLE IP DNSRELAY ↵

Info (1005003): Operation successful.
```

11 DNS リレーの中継先を指定します。通常、中継先には DNS サーバーのアドレスを指定しますが、IPCP によりアドレスを取得するまでは不明であるため、ここではインターフェース名を指定します。

```
Manager > SET IP DNSRELAY INT=ppp0 ↵

Info (1005003): Operation successful.
```

●ファイアウォールの設定

12 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

13 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

14 ICMPパケットはPing（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*1

```
Manager > ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

15 本製品のidentプロキシー機能を無効にし、外部のメール（SMTP）サーバーなどからのident要求に対して、ただちにTCP RSTを返すよう設定します。

```
Manager > DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

16 ファイアウォールポリシーの適用対象となるインターフェースを指定します。LAN側（vlan1）インターフェースをPRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

WAN側（ppp0）インターフェースをPUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

17 LAN側ネットワークに接続されているすべてのコンピューターがENAT機能を使用できるよう設定します。グローバルアドレスには、ppp0のIPアドレスを使用します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=ppp0 ↵

Info (1077003): Operation successful.
```

● DHCPサーバーの設定

18 LAN側コンピューター（DHCPクライアント）のために、DHCPサーバー機能を有効にします。

```
Manager > ENABLE DHCP ↵

Info (1070003): Operation successful.
```

19 DHCPポリシー「BASE」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。IPアドレスの使用期限は7,200秒（2時間）とします。

```
Manager > CREATE DHCP POLICY=BASE
    LEASETIME=7200 ↵

Info (1070003): Operation successful.
```

20 DHCPクライアントに提供する情報を設定します。
ここでは、DNSサーバーアドレスとして、本製品のLAN側インターフェースのIPアドレスを指定しています。

```
Manager > ADD DHCP POLICY=BASE
    SUBNET=255.255.255.0 ROUTER=192.168.2.1
    DNSSERVER=192.168.2.1 ↵

Info (1070003): Operation successful.
```

21 DHCPのレンジ「LOCAL」を作成し、DHCPクライアントに提供するIPアドレスの範囲を設定します。レンジの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE DHCP RANGE=LOCAL POLICY=BASE
    IP=192.168.2.100 NUMBER=32 ↵

Info (1070003): Operation successful.
```

*1 デフォルト設定では、ICMPはファイアウォールを通過できません。

●時刻、パスワード、設定保存

22 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=01-APR-2005 ↵

System time is 01:00:01 on Sunday 01-APR-2005.
```

23 ユーザー「manager」のパスワードを変更します。Confirm：の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↵

Old password: friend ↵
New password: xxxxxxx ↵
Confirm: xxxxxxx ↵
```

24 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

25 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

●接続の確認

26 PPP の接続の確立は、「SHOW PPP」コマンドで確認できます。。

```
Manager > SHOW PPP ↵

 Name          Enabled  ifIndex  Over              CP          State
 ---------------------------------------------------------------------------
 ppp0            YES      04                       IPCP        OPENED
                                 eth0-any          LCP         OPENED
 ---------------------------------------------------------------------------
```

また、「SHOW INT」コマンドでは、全インターフェースの状態を確認できます。

```
Manager > SHOW INT ↵

 Interfaces                                  sysUpTime:         01:26:55

 DynamicLinkTraps.....Disabled
 TrapLimit...........20

 Number of unencrypted PPP/FR links.....1

 ifIndex Interface     ifAdminStatus   ifOperStatus     ifLastChange
 ------------------------------------------------------------------------------
  1       eth0          Up              Up                          01:17:13
  3       vlan1         Up              Up                          00:00:01
  4       ppp0          Up              Up                          01:17:35
 ------------------------------------------------------------------------------

.........
```

27 PPP 接続時にプロバイダーから取得した IP アドレスなどの情報は、「SHOW PPP CONFIG」コマンドによって確認できます。

```
Manager > SHOW PPP CONFIG ↵

 Interface - description
   Parameter                        Configured                Negotiated
 ----------------------------------------------------------------------------
 ppp0 -
                                                         Local           Peer
   .......                               ....
   .......                               ....
 eth0-any
   .......                               ....
   .......                               ....
 IP
   IP Compression Protocol               NONE            NONE             VJC
   IP Pool                            NOT SET
   IP Address Request                      ON
   IP Address                     123.45.11.22    123.45.11.22    123.45.67.1
   Primary DNS Address             87.65.43.21     87.65.43.21           NONE
   Secondary DNS Address           87.65.43.22     87.65.43.22           NONE
   Primary WinS Address               NOT SET                            NONE
   Secondary WinS Address             NOT SET                            NONE
 PPPoE
   Session ID                                            B1CC            B1CC
   MAC Address of Peer                                      00-90-99-0a-0a-04
   Service Name                           any
 Debug
   Maximum packet bytes to display         32
 ----------------------------------------------------------------------------
```

28 LAN 側のコンピューターで Web ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合（DHCP クライアントである場合）、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

まとめ

前述の設定手順を実行することによって、作成、保存されるスクリプトファイルを示します。

表 13.2.3 設定スクリプトファイル（ROUTER.CFG）

1	CREATE PPP=0 OVER=eth0-any
2	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
3	ENABLE IP
4	ENABLE IP REMOTEASSIGN
5	ADD IP INT=vlan1 IP=192.168.2.1 MASK=255.255.255.0
6	ADD IP INT=ppp0 IP=0.0.0.0
7	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
8	ENABLE IP DNSRELAY
9	SET IP DNSRELAY INT=ppp0
10	ENABLE FIREWALL
11	CREATE FIREWALL POLICY=net
12	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
13	DISABLE FIREWALL POLICY=net IDENTPROXY
14	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
15	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
16	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
17	ENABLE DHCP
18	CREATE DHCP POLICY=BASE LEASETIME=7200
19	ADD DHCP POLICY=BASE SUBNET=255.255.255.0 ROUTER=192.168.2.1 DNSSERVER=192.168.2.1
20	CREATE DHCP RANGE=LOCAL POLICY=BASE IP=192.168.2.100 NUMBER=32

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

13.3 PPPoE による LAN 型インターネット接続（アンナンバード）

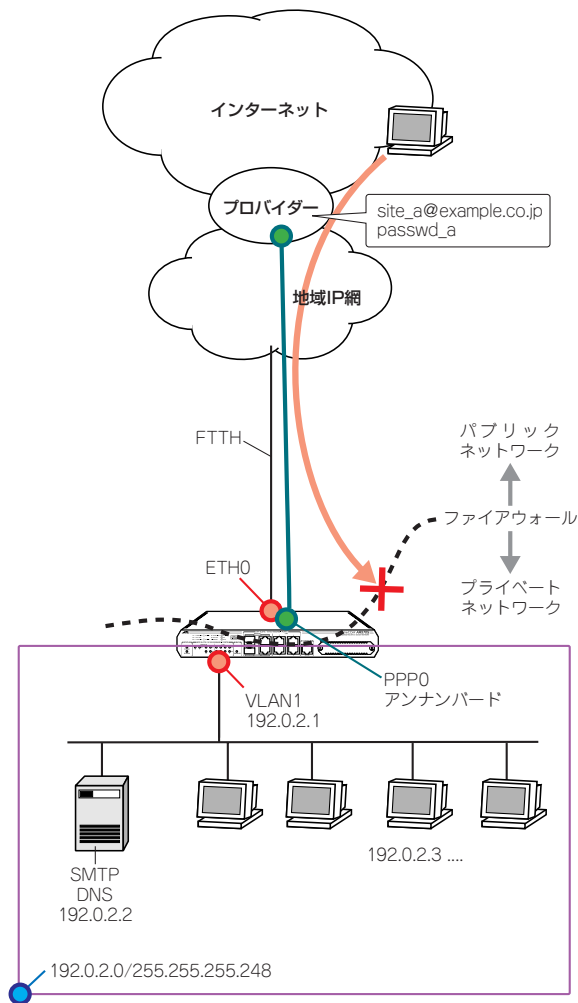



図 13.3.1 PPPoE による LAN 型の接続（LAN 側グローバル）

PPPoE を使ってプロバイダーに接続します。グローバルアドレスを 8 個、16 個などのブロック単位で固定的に割り当てられる LAN 型接続の設定例です。

この例では、NAT を使用せず、LAN 側端末にグローバルアドレスを直接割り当てます。また、ファイアウォールを使って外部からのアクセスを原則拒否しつつ、特定のサーバーだけを外部に公開します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- 使用できる IP アドレス：192.0.2.0/29（192.0.2.0 〜 192.0.2.7）

設定の方針

- LAN 側端末はすべてグローバルアドレスで運用します。NAT は使用しません。プロバイダーから割り当てられているアドレスは 8 個ですが、ネットワークアドレス（192.0.2.0）、ブロードキャストアドレス（192.0.2.7）、ルーター自身のアドレス（192.0.2.1）にそれぞれ 1 個ずつ消費されるため、端末に設定できるアドレスは 192.0.2.2 〜 192.0.2.6 の 5 個となります。

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。

- 外部からのアクセスは基本的にすべて遮断しますが、次のサービスだけは特例として許可します。
  - SMTP サーバー：192.0.2.2：25/tcp
  - DNS サーバー：192.0.2.2：53/tcp、53/udp

- 本製品の基本設定は、次の通りです。

表 13.3.1 本製品の基本設定

WAN 側物理インターフェース	eth0
WAN 側（ppp0）IP アドレス	アンナンバード
LAN 側（VLAN1）IP アドレス	192.0.2.1/24
DHCP サーバー機能	使わない

設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend （表示されません）
```

●PPP の設定

3 WAN 側 Ethernet インターフェース（eth0）上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

4 プロバイダーから通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視し、自動的に PPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=site_a@example.co.jp
    PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

アンナンバードによる WAN 側インターフェースに関しては下記の項もご覧ください。

参照 本書「PPPoE におけるアンナンバード」（p.128）

●IP、ルーティングの設定

5 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

6 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するように設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.
```

7 LAN側（vlan1）インターフェースにISPから割り当てられたグローバルアドレスの先頭アドレス（192.0.2.1）を設定します。アドレスを8個や16個といった単位で割り当てられる場合は、ネットマスクが変則的になるので注意してください。

```
Manager > ADD IP INT=vlan1 IP=192.0.2.1
    MASK=255.255.255.248 ↵

Info (1005275): interface successfully added.
```

8 WAN側（ppp0）インターフェースをアンナンバードに設定します。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

9 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

10 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

11 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

12 ICMPパケットはPing（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*2

```
Manager > ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

*2 デフォルト設定では、ICMPはファイアウォールを通過できません。

13 外部のメール（SMTP）サーバーなどからのident要求に対して、本製品が内部のサーバーの代わりに応答する、identプロキシー機能がデフォルトで有効になっています。そこで、内部のサーバー自身が応答できるように、identプロキシー機能を無効にします。

```
Manager > DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

14 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN側（VLAN1）インターフェースをPRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=VLAN1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

WAN側（ppp0）インターフェースをPUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

15 外部からのパケットをすべて拒否するファイアウォールの基本ルールに対し、DMZのサーバーへパケットを通すための設定を行います。

SMTPサーバー（192.0.2.2のTCP25番）へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=1
    AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.2
    PORT=25 ↵

Info (1077003): Operation successful.
```

DNS サーバー（192.0.2.2 の TCP[*3] と UDP の 53 番）へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=2
    AC=ALLOW INT=ppp0-0 PROTO=TCP IP=192.0.2.2
    PORT=53 ↵

Info (1077003): Operation successful.

Manager > ADD FIREWALL POLICY=net RULE=2
    AC=ALLOW INT=ppp0-0 PROTO=UDP IP=192.0.2.2
    PORT=53 ↵

Info (1077003): Operation successful.
```

●時刻、パスワード、設定保存

16 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=01-APR-2005 ↵

System time is 01:00:01 on Sunday 01-APR-2005.
```

17 ユーザー「manager」のパスワードを変更します。Confirm：の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↵

Old password: friend ↵
New password: xxxxxxx ↵
Confirm: xxxxxxx ↵
```

18 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

19 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

*3 セカンダリーDNS サーバーからのアクセスで TCP が使用されます。

●接続の確認

20 PPP の接続の確立は、「SHOW PPP」コマンドで確認できます。

```
Manager > SHOW PPP ↵

 Name          Enabled  ifIndex  Over                CP          State
 ------------------------------------------------------------------------
 ppp0            YES      04                         IPCP        OPENED
                                 eth0-any            LCP         OPENED
 ------------------------------------------------------------------------
```

また、「SHOW INT」コマンドでは、全インターフェースの状態を確認できます。

```
Manager > SHOW INT ↵

 Interfaces                                sysUpTime:          01:26:55

 DynamicLinkTraps.....Disabled
 TrapLimit...........20

 Number of unencrypted PPP/FR links.....1

 ifIndex Interface     ifAdminStatus   ifOperStatus     ifLastChange
 -------------------------------------------------------------------------
  1      eth0          Up              Up                   01:17:13
  3      vlan1         Up              Up                   00:00:01
  4      ppp0          Up              Up                   01:17:35
 -------------------------------------------------------------------------

.........
```

21 PPP 接続時にプロバイダーから取得した IP アドレスなどの情報は、「SHOW PPP CONFIG」コマンドによって確認できます。

```
Manager > SHOW PPP CONFIG ↵

 Interface - description
   Parameter                   Configured               Negotiated
 ------------------------------------------------------------------------
 ppp0 -
                                                    Local          Peer
   .......                           ....
   .......                           ....
 eth0-any
   .......                           ....
   .......                           ....
 IP
   IP Compression Protocol           NONE           NONE           VJC
   IP Pool                        NOT SET
   IP Address Request                  ON
   IP Address                 123.45.11.22   123.45.11.22    123.45.67.1
   Primary DNS Address         87.65.43.21    87.65.43.21           NONE
   Secondary DNS Address       87.65.43.22    87.65.43.22           NONE
   Primary WinS Address           NOT SET                           NONE
   Secondary WinS Address         NOT SET                           NONE
 PPPoE
   Session ID                                       B1CC            B1CC
   MAC Address of Peer                                 00-90-99-0a-0a-04
   Service Name                       any
 Debug
   Maximum packet bytes to display     32
 ------------------------------------------------------------------------
```

22 LAN 側のコンピューターでWeb ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合（DHCP クライアントである場合）、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 13.3.2 設定スクリプトファイル（ROUTER.CFG）

1	CREATE PPP=0 OVER=eth0-any
2	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
3	ENABLE IP
4	ENABLE IP REMOTEASSIGN
5	ADD IP INT=VLAN1 IP=192.0.2.1 MASK=255.255.255.248
6	ADD IP INT=ppp0 IP=0.0.0.0
7	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
8	ENABLE FIREWALL
9	CREATE FIREWALL POLICY=net
10	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
11	DISABLE FIREWALL POLICY=net IDENTPROXY
12	ADD FIREWALL POLICY=net INT=VLAN1 TYPE=PRIVATE
13	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
14	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.2 PORT=25
15	ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.2 PORT=53
16	ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0 PROTO=UDP IP=192.0.2.2 PORT=53

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

13.4 PPPoE による LAN 型インターネット接続（DMZ の設定）

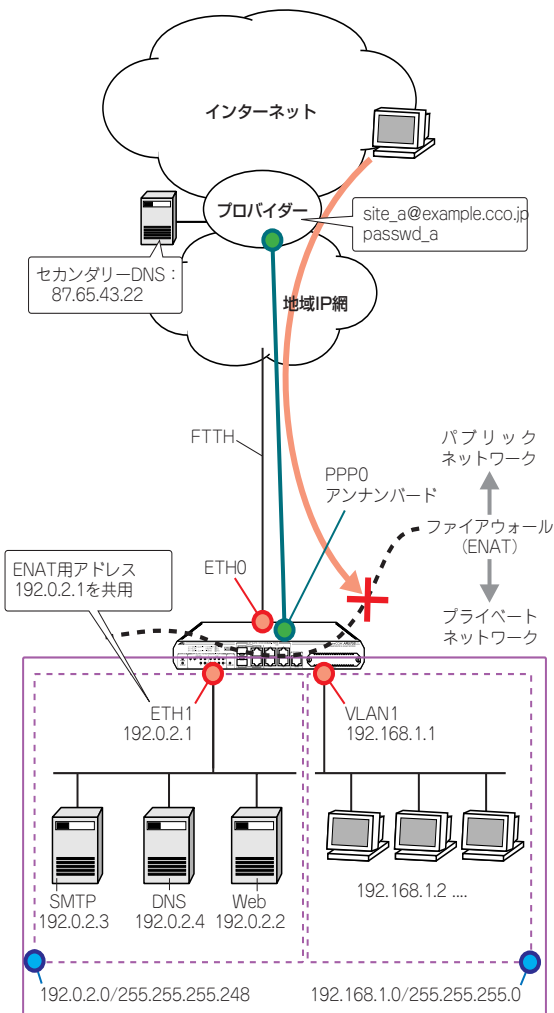



図 13.4.1 PPPoE による LAN 型の接続（DMZ）

PPPoE を使ってプロバイダーに接続します。グローバルアドレスを 8 個、16 個などのブロック単位で固定的に割り当てられる LAN 型接続の設定例です。

この例では、LAN 側を 2 つのサブネットに分割し、一方をグローバルアドレスで運用するサーバー用（DMZ）、もう一方をプライベートアドレスで運用するクライアント用とします。クライアントはダイナミック ENAT 経由でインターネットにアクセスします。また、ファ

イアウォールを使って外部からのアクセスを原則拒否しつつ、特定のサーバーだけを外部に公開します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- 使用できる IP アドレス：192.0.2.0/29（192.0.2.0 ～ 192.0.2.7）

設定の方針

- LAN 側を vlan1 と eth1 の 2 つのサブネットに分割し、eth1 にはプロバイダーから割り当てられたグローバルアドレスを、vlan1 にはプライベートアドレスを割り当てます。グローバルサブネットは DMZ としてサーバーを配置し、プライベートサブネットにはクライアントを配置します。

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。

- 外部からのアクセスは基本的にすべて遮断しますが、次のサービスだけは特例として許可します。
  - Web サーバー：192.0.2.2：80/tcp
  - SMTP サーバー：192.0.2.3：25/tcp
  - DNS サーバー：192.0.2.4：53/tcp、53/udp

- プライベートサブネットのクライアントがインターネットにアクセスできるよう、ダイナミックENAT を使用します。グローバルアドレスには、eth1 に割り当てたアドレス（192.0.2.1）を共用します。

- 本製品の基本設定は、次の通りです。

表 13.4.1 本製品の基本設定

WAN 側物理インターフェース	eth0
WAN 側（ppp0）IP アドレス	アンナンバード
DMZ 側（eth1）IP アドレス	192.0.2.1/29
LAN 側（vlan1）IP アドレス	192.168.1.1/24
DHCP サーバー機能	使わない

設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

●PPP の設定

3 WAN 側 Ethernet インターフェース（eth0）上にPPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

4 プロバイダーから通知されたPPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視し、自動的に PPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=site_a@example.co.jp
    PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

アンナンバードによるWAN 側インターフェースに関しては下記の項もご覧ください。

参照 本書「PPPoE におけるアンナンバード」（p.128）

●IP、ルーティングの設定

5 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

6 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するように設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.
```

7 DMZ 側（eth1）インターフェースにプロバイダーから割り当てられたグローバルアドレスの先頭アドレス（192.0.2.1）を設定します。アドレスを 8 個や 16 個といった単位で割り当てられる場合は、ネットマスクが変則的になるので注意してください。

```
Manager > ADD IP INT=eth1 IP=192.0.2.1
    MASK=255.255.255.248 ↵

Info (1005275): interface successfully added.
```

8 LAN 側（vlan1）インターフェースにプライベート IP アドレスを割り当て、クライアント用のサブネットとします。

```
Manager > ADD IP INT=vlan1 IP=192.168.1.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

9 WAN 側（ppp0）インターフェースをアンナンバードに設定します。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

10 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

11 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

12 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

13 ICMP パケットは Ping（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*4

```
Manager > ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

14 外部のメール(SMTP) サーバーなどからのident 要求に対して、本製品が内部のサーバーの代わりに応答する、ident プロキシー機能がデフォルトで有効になっています。そこで、内部のサーバー自身が応答できるように、ident プロキシー機能を無効にします。

```
Manager > DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

15 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

DMZ 側（eth1）インターフェースを PRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=eth1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

LAN 側（vlan1）インターフェースを PRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

*4 デフォルト設定では、ICMP はファイアウォールを通過できません。

WAN 側（ppp0）インターフェースを PUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

16 LAN 側（vlan1）ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。グローバルアドレスには 192.0.2.1 を共用します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=ppp0 GBLIP=192.0.2.1 ↵

Info (1077003): Operation successful.
```

17 外部からのパケットをすべて拒否するファイアウォールの基本ルールに対し、DMZ のサーバーへパケットを通すための設定を行います。

Web サーバー（192.0.2.2 の TCP80 番）へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=1
    AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.2
    PORT=80 ↵

Info (1077003): Operation successful.
```

SMTP サーバー（192.0.2.3 の TCP25 番）へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=2
    AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.3
    PORT=25 ↵

Info (1077003): Operation successful.
```

DNS サーバー（192.0.2.4 の TCP*5 と UDP の 53 番）へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=3
    AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.4
    PORT=53 ↵

Info (1077003): Operation successful.

Manager > ADD FIREWALL POLICY=net RULE=4
    AC=ALLOW INT=ppp0 PROTO=UDP IP=192.0.2.4
    PORT=53 ↵

Info (1077003): Operation successful.
```

●時刻、パスワード、設定保存

18 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=01-APR-2005 ↵

System time is 01:00:01 on Sunday 01-APR-2005.
```

19 ユーザー「manager」のパスワードを変更します。Confirm：の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↵

Old password: friend ↵
New password: xxxxxxx ↵
Confirm: xxxxxxx ↵
```

20 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

21 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

*5 セカンダリー DNS サーバーからのアクセスで TCP が使用されます。

●接続の確認

22 PPPの接続の確立は、「SHOW PPP」コマンドで確認できます。

```
Manager > SHOW PPP ↵

  Name           Enabled  ifIndex  Over                  CP          State
  ---------------------------------------------------------------------------
  ppp0             YES      04                           IPCP        OPENED
                                   eth0-any              LCP         OPENED
  ---------------------------------------------------------------------------
```

また、「SHOW INT」コマンドでは、全インターフェースの状態を確認できます。

```
Manager > SHOW INT ↵

  Interfaces                                  sysUpTime:          01:26:55

  DynamicLinkTraps.....Disabled
  TrapLimit............20

  Number of unencrypted PPP/FR links.....1

  ifIndex Interface     ifAdminStatus  ifOperStatus     ifLastChange
  ----------------------------------------------------------------------------
   1      eth0          Up             Up                         01:17:13
   3      vlan1         Up             Up                         00:00:01
   4      ppp0          Up             Up                         01:17:35
  ----------------------------------------------------------------------------

.........
```

23 PPP接続時にプロバイダーから取得したIPアドレスなどの情報は、「SHOW PPP CONFIG」コマンドによって確認できます。

```
Manager > SHOW PPP CONFIG ↵

  Interface - description
    Parameter                      Configured                Negotiated
  --------------------------------------------------------------------------
  ppp0 -
                                                       Local            Peer
    .......                           ....
    .......                           ....
  eth0-any
    .......                           ....
    .......                           ....
  IP
    IP Compression Protocol           NONE            NONE              VJC
    IP Pool                        NOT SET
    IP Address Request                  ON
    IP Address                123.45.11.22    123.45.11.22      123.45.67.1
    Primary DNS Address        87.65.43.21     87.65.43.21             NONE
    Secondary DNS Address      87.65.43.22     87.65.43.22             NONE
    Primary WinS Address           NOT SET                             NONE
    Secondary WinS Address         NOT SET                             NONE
  PPPoE
    Session ID                                    B1CC             B1CC
    MAC Address of Peer                              00-90-99-0a-0a-04
    Service Name                       any
  Debug
    Maximum packet bytes to display     32
  --------------------------------------------------------------------------
```

24 LAN側のコンピューターでWebブラウザーなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN側のコンピューターがIPアドレスを自動取得するように設定されている場合（DHCPクライアントである場合）、本製品のDHCPサーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表13.4.2 設定スクリプトファイル（ROUTER.CFG）

1	CREATE PPP=0 OVER=eth0-any
2	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
3	ENABLE IP
4	ENABLE IP REMOTEASSIGN
5	ADD IP INT=eth1 IP=192.0.2.1 MASK=255.255.255.248
6	ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0
7	ADD IP INT=ppp0 IP=0.0.0.0
8	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
9	ENABLE FIREWALL
10	CREATE FIREWALL POLICY=net
11	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
12	DISABLE FIREWALL POLICY=net IDENTPROXY
13	ADD FIREWALL POLICY=net INT=eth1 TYPE=PRIVATE
14	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
15	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
16	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0 GBLIP=192.0.2.1
17	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.2 PORT=80
18	ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.3 PORT=25
19	ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.4 PORT=53
20	ADD FIREWALL POLICY=net RULE=4 AC=ALLOW INT=ppp0 PROTO=UDP IP=192.0.2.4 PORT=53

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

13.5 Ethernet による端末型インターネット接続

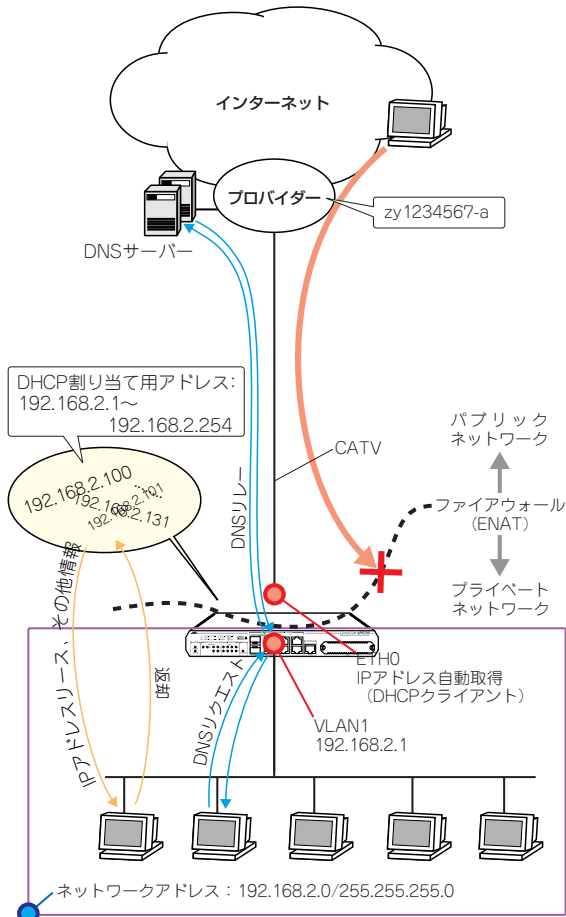



図 13.5.1 CATV による端末型の接続

CATV 系でよく見られる接続形態です。ケーブルモデムを介して、Ethernet でプロバイダーに接続します。この例は、DHCP によりグローバル IP アドレスを動的に割り当てられる端末型接続の基本設定です。

ダイナミック ENAT で 1 個のアドレスを共用し、ファイアウォールで外部からの不正アクセスを防止します。また、LAN 側クライアントの設定を簡単にするため、DNS リレーと DHCP サーバーも利用します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。「コンピューター名」は、接続の際の認証に使用される文字列です（コンピューター名が提供されないプロバイダーもあります。その場合、設定は不要です）。

- コンピューター名：zy1234567-a
- IP アドレス グローバルアドレス：1 個（動的割り当て）
- ゲートウェイアドレス：接続時に通知される
- DNS サーバー：接続時に通知される

設定の方針

- WAN 側 Ethernet インターフェースの IP アドレスとネットマスクは、プロバイダーの DHCP サーバーから取得します。また、ゲートウェイアドレスと DNS サーバーアドレスも、DHCP サーバーから入手し自動的に設定します。

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。

- ファイアウォールのダイナミック ENAT 機能を使用して、LAN 側ネットワークのプライベート IP アドレスを、プロバイダーから与えられたグローバル IP アドレスに変換します。これにより、LAN に接続された複数のコンピューターからインターネットへの同時アクセスが可能になります。

- 本製品の IP アドレスは、下記のように設定します。

表 13.5.1 本製品の基本設定

WAN 側（eth0）IP アドレス	接続時にプロバイダーの DHCP サーバーから取得する
LAN 側（vlan1）IP アドレス	192.168.2.1/24
DHCP サーバー機能	有効

- 本製品を DHCP サーバーとして動作させ、LAN に接続されたコンピューターに IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバーアドレスの情報を提供します。

表 13.5.2 本製品のDHCP サーバーの設定

DHCP ポリシー名	BASE
使用期限	7200（秒）
サブネットマスク	255.255.255.0
デフォルトルート	192.168.2.1
DNS サーバー	192.168.2.1
DHCP レンジ名	LOCAL
提供する IP アドレスの範囲	192.168.2.100 ～ 192.168.2.131（32 個）

- 本製品のDNS リレー機能をオンにして、LAN 側コンピューターからの DNS リクエストを、プロバイダーの DNS サーバーに転送します。上記 DHCP サーバーの設定により、LAN側コンピューターに対しては、DNS サーバーアドレスとして本製品自身の IP アドレスを教えます。

設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

● IP、ルーティングの設定

3 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

4 プロバイダーの DHCP サーバーから取得した IP アドレスを、WAN 側（eth0）インターフェースに割り当てるよう設定します。また、デフォルトルート、DNS サーバーアドレスの設定も、DHCP サーバーからの情報に基づいて自動的に行われます。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.

Manager > ADD IP INT=eth0 IP=DHCP ↵

Info (1005275): interface successfully added.
```

5 LAN 側（vlan1）インターフェースに IP アドレスを設定します。

```
Manager > ADD IP INT=vlan1 IP=192.168.2.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

● DNS リレーの設定

6 DNS リレー機能を有効にします。

```
Manager > ENABLE IP DNSRELAY ↵

Info (1005003): Operation successful.
```

●ファイアウォールの設定

7 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

8 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

9 ICMP パケットは Ping（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*6

```
Manager > ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

10 本製品のident プロキシー機能を無効にし、外部のメール（SMTP）サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager > DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

*6 デフォルト設定では、ICMP はファイアウォールを通過できません。

11 ファイアウォールポリシーの適用対象となるインターフェースを指定します。LAN 側（vlan1）インターフェースを PRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↲

Info (1077003): Operation successful.
```

WAN 側（eth0）インターフェースをPUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=eth0
    TYPE=PUBLIC ↲

Info (1077003): Operation successful.
```

12 LAN 側ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。グローバルアドレスには、WAN 側（eth0）インターフェースの IP アドレスを使用します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=eth0 ↲

Info (1077003): Operation successful.
```

●DHCP サーバーの設定

13 LAN 側コンピューター（DHCP クライアント）のために、DHCP サーバー機能を有効にします。

```
Manager > ENABLE DHCP ↲

Info (1070003): Operation successful.
```

14 DHCP ポリシー「BASE」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。IP アドレスの使用期限は 7,200 秒（2 時間）とします。

```
Manager > CREATE DHCP POLICY=BASE
    LEASETIME=7200 ↲

Info (1070003): Operation successful.
```

15 DHCP クライアントに提供する情報を設定します。
ここでは、DNS サーバーアドレスとして、本製品のLAN 側インターフェースの IP アドレスを指定しています。

```
Manager > ADD DHCP POLICY=BASE
    SUBNET=255.255.255.0 ROUTER=192.168.2.1
    DNSSERVER=192.168.2.1 ↲

Info (1070003): Operation successful.
```

16 DHCP のレンジ「LOCAL」を作成し、DHCP クライアントに提供する IP アドレスの範囲を設定します。レンジの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE DHCP RANGE=LOCAL POLICY=BASE
    IP=192.168.2.100 NUMBER=32 ↲

Info (1070003): Operation successful.
```

●接続認証の設定

17 プロバイダーからコンピューター名が指示されている場合、そのコンピュータ名ーを本製品のシステム名に設定します（大文字・小文字を判別しますので、正確に入力してください）。システム名に設定された文字列は、本製品がプロバイダーの DHCP サーバーに対して、IP アドレスを要求する際の認証の文字列として使用されます。

```
Manager > SET SYSTEM NAME=zy1234567-a ↲
```

●時刻、パスワード、設定保存

18 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager zy1234567-a> SET TIME=01:00:01
    DATE=01-APR-2005 ↲

System time is 01:00:01 on Sunday 01-APR-2005.
```

19 ユーザー「manager」のパスワードを変更します。Confirm：の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager zy1234567-a> SET PASSWORD ↲

Old password: friend ↲
New password: xxxxxxx ↲
Confirm: xxxxxxx ↲
```

20 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager zy1234567-a> CREATE CONF=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

21 起動スクリプトとして指定します。

```
Manager zy1234567-a> SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

●接続の確認

22 接続時にプロバイダーから取得した IP アドレスなどの情報は、「SHOW DHCP」コマンドによって確認できます。

```
Manager zy1234567-a> SHOW DHCP ↵

DHCP Server

  State ................. enabled
  BOOTP Status ........... disabled
  Debug Status ........... disabled
  Policies ............... BASE
  Ranges ................. LOCAL ( 192.168.2.100 - 192.168.2.131 )
  In Messages ............ 6
  Out Messages ........... 10
  In DHCP Messages ....... 6
  Out DHCP Messages ...... 10
  In BOOTP Messages ...... 0
  Out BOOTP Messages ..... 0

DHCP Client

  Interface ............. eth0
  State ................. bound
  Server ................ 123.45.11.5
  Assigned Domain ........ myisp.ne.jp
  Assigned IP ............ 123.45.11.22
  Assigned Mask .......... 255.255.255.0
  Assigned Gateway ....... 123.45.11.1
  Assigned DNS ........... 87.65.43.21 87.65.43.22
  Assigned Lease ......... 259200
```

23 LAN 側のコンピューターで Web ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合（DHCP クライアントである場合）、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

まとめ

前述の設定手順を実行することによって、作成、保存されるスクリプトファイルを示します。

表 13.5.3 設定スクリプトファイル（ROUTER.CFG）

1	ENABLE IP
2	ENABLE IP REMOTEASSIGN
3	ADD IP INT=eth0 IP=DHCP
4	ADD IP INT=vlan1 IP=192.168.2.1 MASK=255.255.255.0
5	ENABLE IP DNSRELAY
6	ENABLE FIREWALL
7	CREATE FIREWALL POLICY=net
8	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
9	DISABLE FIREWALL POLICY=net IDENTPROXY
10	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
11	ADD FIREWALL POLICY=net INT=eth0 TYPE=PUBLIC
12	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=eth0
13	ENABLE DHCP
14	CREATE DHCP POLICY=BASE LEASETIME=7200
15	ADD DHCP POLICY=BASE SUBNET=255.255.255.0 ROUTER=192.168.2.1 DNSSERVER=192.168.2.1
16	CREATE DHCP RANGE=LOCAL POLICY=BASE IP=192.168.2.100 NUMBER=32
17	SET SYSTEM NAME=zy1234567-a

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

13.6 インターネット接続による２点間 IPsec VPN

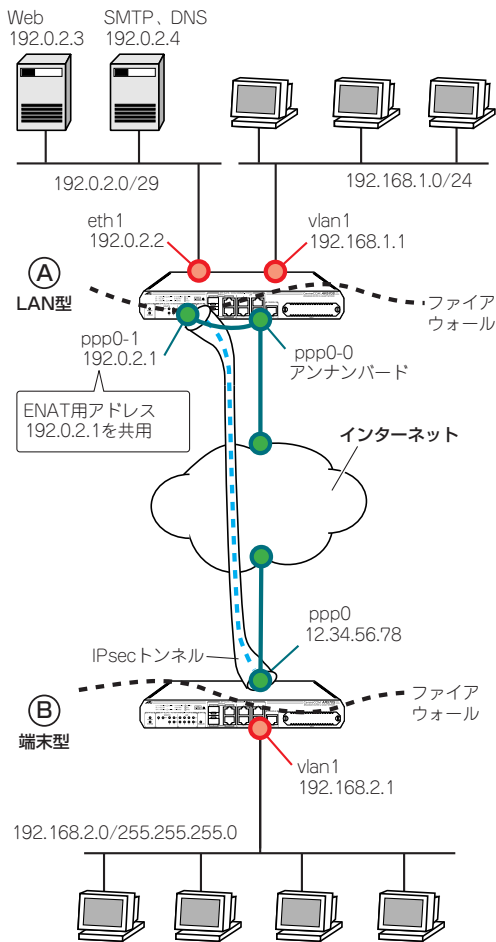



図 13.6.1 IPsec による接続

PPPoE でインターネットに接続している 2 つの拠点を、IPsec で接続しデータの安全性を確保します。

この例では、以下の 2 拠点間の接続を、トンネルモード（ESP）で暗号化します。

- グローバルアドレス 8 個を固定的に割り当てられている拠点 A
- グローバルアドレス 1 個を固定的に割り当てられている拠点 B

上記の組み合わせ以外に対しても、本設定例中の IPsec 部分の適用は可能ですが、最低限一方の IP アドレスが固定である必要があります。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●拠点 A

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：192.0.2.0/29（8 個固定）
- DNS サーバー：接続時に通知される

●拠点 B

- 接続のユーザー名：site_b@example.co.jp
- 接続のパスワード：passswd_b
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：12.34.56.78/32（1 個固定）
- DNS サーバー：接続時に通知される

設定の方針

●インターネット接続設定

- グローバルアドレス 8 個をもつ拠点 A のルーターでは、グローバルサブネット（eth1）にサーバーを、プライベートサブネット（vlan1）にクライアントを配置します。また、WAN 側（ppp0）インターフェースをマルチホーミングし、そのうちの一方（ppp0-1）にグローバルアドレスの 1 つを設定します。拠点 A のルーターが送信する IPsec パケットの始点アドレスにはこのアドレスがセットされます。
  このような設定をするのは、PPPoE の LAN 型接続では WAN 側（ppp0）インターフェースにネットワークアドレス（ホスト部が 0 のアドレスが始点アドレスとしては使用できないため事実上のアンナンバード）が割り当てられるためです

- グローバルアドレスが 1 個しかない拠点 B のルーターでは、WAN 側（ppp0）インターフェースにグローバルアドレスを設定したダイナミック ENAT による、通常の端末型を使用します。このグローバルアドレスが IPsec パケットの始点アドレスとしてセットされます。

表 13.6.1 インターネット接続設定

	拠点 A	拠点 B
WAN 側物理インターフェース	eth0	eth0
WAN 側 IP アドレス（1）	Unnumbered（ppp0-0）	12.34.56.78/32（ppp0）
WAN 側 IP アドレス（2）	192.0.2.1/32（ppp0-1）	-
LAN 側IP アドレス	192.168.1.1/24（vlan1）	192.168.2.1/24（vlan1）
DMZ 側 IP アドレス	192.0.2.2/29（eth1）	-

● VPN 設定

- IPsec トンネルは、A の ppp0-1 と B の ppp0 の間に張られます。このトンネルはプライベートLAN 間を接続するためのもので、IP のパケットを暗号化して通します。
- ファイアウォールの設定においては、IPsec関連のパケット（IKE、ESP）を除く外部からの不正アクセスを遮断し､内部からは自由にインターネットへのアクセスができるようにします。
- トンネリング対象のパケットにNAT が適用されないようルールを設定します。

表 13.6.2 IKE フェーズ 1（ISAKMP SA のネゴシエーション）

本製品間の認証方式	事前共有鍵（pre-shared key）
IKE 交換モード	Main モード
事前共有鍵	secret（文字列）
Oakley グループ	1（デフォルト）
ISAKMP メッセージの暗号化方式	DES（デフォルト）
ISAKMP メッセージの認証方式	SHA1（デフォルト）
ISAKMP SA の有効期限（時間）	86400 秒（24 時間）（デフォルト）
ISAKMP SA の有効期限（Kbyte 数）	なし（デフォルト）
起動時の ISAKMP ネゴシエーション	行わない

表 13.6.3 IKE フェーズ 2（IPsec SA のネゴシエーション）

SA モード	トンネルモード
セキュリティープロトコル	ESP（暗号＋認証）
暗号化方式	DES
認証方式	SHA1
IPComp	使わない
IPsec SA の有効期限（時間）	28800 秒（8 時間）（デフォルト）
IPsec SA の有効期限（Kbyte 数）	なし（デフォルト）
IPsec の適用対象 IP アドレス	192.168.1.0/24 ⇔ 192.168.2.0/24
トンネル終端アドレス	192.0.2.1 ⇔ 12.34.56.78
インターネットとの平文通信	行なう

拠点 A の設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

3 管理をしやすくするために、本製品にシステム名を設定します。サイトA には「A」を設定します。

```
Manager > SET SYSTEM NAME=A ↵

Info (1034003): Operation successful.

Manager A>
```

4 IPsecはセキュリティーモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officer レベルのユーザーを登録しておきます。Security Officer のパスワードは厳重に管理してください。ここでは、ユーザー名「secoff」、パスワード「passwdSA」を仮定します。

```
Manager A> ADD USER=secoff PASSWORD=passwdSA
    PRIVILEGE=SECURITYOFFICER ↵

User Authentication Database
-----------------------------------------------------------------------------
Username: secoff ()
   Status: enabled    Privilege: Sec Off   Telnet: no    Login: yes
   Logins: 0          Fails: 0        Sent: 0           Rcvd: 0
   Authentications: 0 Fails: 0
-----------------------------------------------------------------------------
```

●PPPの設定

5 WAN側Ethernetインターフェース（eth0）上にPPPインターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知されたPPPoEの「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager A> CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

6 プロバイダーから通知されたPPPユーザー名とパスワードを指定し、接続時にIPアドレス割り当ての要求を行うように設定します。LQRはオフにし、代わりにLCP Echoパケットを使ってPPPリンクの状態を監視し、自動的にPPPoEのセッションを再接続するようにします（セッションキープアライブ）。また、ISDN向けの機能であるBAPはオフにします。

```
Manager A> SET PPP=0 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=site_a@example.co.jp
    PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

●IP、ルーティングの設定

7 IPモジュールを有効にします。

```
Manager A> ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

8 IPCPネゴシエーションで与えられたIPアドレスをPPPインターフェースで使用するように設定します。

```
Manager A> ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.
```

9 DMZ側（eth1）インターフェースにプロバイダーから割り当てられたグローバルアドレスのうちの1つ 192.0.2.2 を設定します。アドレスを8個や16個といった単位で割り当てられる場合は、ネットマスクが変則的になるので注意してください。

```
Manager A> ADD IP INT=eth1 IP=192.0.2.2
    MASK=255.255.255.248 ↵

Info (1005275): interface successfully added.
```

10 LAN側（vlan1）インターフェースにプライベートIPアドレスを割り当て、クライアント用のサブネットとします。

```
Manager A> ADD IP INT=vlan1 IP=192.168.1.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

11 WAN側（ppp0）インターフェースをマルチホーミングし、ppp0-0をアンナンバードに設定します。

```
Manager A> ADD IP INT=ppp0-0 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

12 WAN側（ppp0-1）インターフェースにプロバイダーから割り当てられたグローバルアドレスの先頭アドレス（192.0.2.1）を32ビットマスクで割り当てます。デフォルトルートをこのインターフェースに向けることで、IPsecパケットの始点アドレスとしてこのアドレスが使われるようにします

```
Manager A> ADD IP INT=ppp0-1 IP=192.0.2.1
    MASK=255.255.255.255 ↵

Info (1005275): interface successfully added.
```

13 デフォルトルートをppp0-1に向けて設定します。これは、ルーターAが送信するIPsecパケットの始点アドレスとして、ppp0-1のアドレスが使われるようにするためです（通常、本製品自身がパケットを送信するときは、送出インターフェースのアドレスを始点アドレスとして使います）。

```
Manager A> ADD IP ROUTE=0.0.0.0 INT=ppp0-1
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

14 ファイアウォール機能を有効にします。

```
Manager A> ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

15 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager A> CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

16 ICMP パケットは Ping（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*7

```
Manager A> ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

17 外部のメール(SMTP) サーバーなどからのident 要求に対して、本製品が内部のサーバーの代わりに応答する、ident プロキシー機能がデフォルトで有効になっています。そこで、内部のサーバー自身が応答できるように、ident プロキシー機能を無効にします。

```
Manager A> DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

18 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

DMZ 側（eth1）インターフェースを PRIVATE（内部）に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=eth1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

LAN 側（vlan1）インターフェースを PRIVATE（内部）に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

WAN 側（ppp0-1）インターフェースを PUBLIC（外部）に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp0-1
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

WAN 側（ppp0-1）インターフェースを PUBLIC（外部）に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp0-1
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

19 LAN 側（vlan1）ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。グローバルアドレスにはppp0-1に割り当てた192.0.2.1を共用します。

```
Manager A> ADD FIREWALL POLICY=net
    NAT=ENHANCED INT=vlan1 GBLINT=ppp0-1
    GBLIP=192.0.2.1 ↵

Info (1077003): Operation successful.
```

20 外部からのパケットをすべて拒否するファイアウォールの基本ルールに対し、DMZ のサーバーへパケットを通すための設定を行います。

Web サーバー（192.0.2.3 の TCP80 番）へのパケットは通過させます。

```
Manager A> ADD FIREWALL POLICY=net RULE=1
    AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.3
    PORT=80 ↵

Info (1077003): Operation successful.
```

SMTP サーバー（192.0.2.4 の TCP25 番）へのパケットは通過させます。

```
Manager A> ADD FIREWALL POLICY=net RULE=2
    AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4
    PORT=25 ↵

Info (1077003): Operation successful.
```

*7 デフォルト設定では、ICMP はファイアウォールを通過できません。

DNS サーバー（192.0.2.4 の TCP[*8] と UDP の 53 番）へのパケットは通過させます。

```
Manager A> ADD FIREWALL POLICY=net RULE=3
    AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4
    PORT=53 ↵

Info (1077003): Operation successful.

Manager A> ADD FIREWALL POLICY=net RULE=4
    AC=ALLOW INT=ppp0-1 PROTO=UDP IP=192.0.2.4
    PORT=53 ↵

Info (1077003): Operation successful.
```

21 接続相手からの IKE パケット（UDP500 番）がファイアウォールを通過できるように設定します。

```
Manager A> ADD FIREWALL POLICY=net RU=5
    AC=ALLOW INT=ppp0-1 PROTO=UDP GBLPO=500
    GBLIP=192.0.2.1 PO=500 IP=192.0.2.1 ↵

Info (1077003): Operation successful.
```

22 ローカルLAN からリモート LAN へのパケットにはNAT をかけないように設定します。

```
Manager A> ADD FIREWALL POLICY=net RU=6
    AC=NONAT INT=vlan1 PROT=ALL
    IP=192.168.1.1-192.168.1.254 ↵

Info (1077003): Operation successful.

Manager A> SET FIREWALL POLICY=net RU=6
    REMOTEIP=192.168.2.1-192.168.2.254 ↵

Info (1077003): Operation successful.
```

23 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点IP アドレスが 192.168.1.1 ～ 192.168.1.254、つまりローカル LAN 側ならば、NAT の対象外とする」の意味になります。

```
Manager A> ADD FIREWALL POLICY=net RU=7
    AC=NONAT INT=ppp0-1 PROT=ALL
    IP=192.168.1.1-192.168.1.254 ENCAP=IPSEC ↵

Info (1077003): Operation successful.
```

*8 セカンダリーDNS サーバーからのアクセスで TCP が使用されます。

● IPsec の設定

24 ここからが IPsec の設定になります。最初にISAKMP 用の事前共有鍵（pre-shared key）を作成します。ここでは鍵番号を 1 番とし、鍵の値は「secret」という文字列で指定します（拠点 B のルーターも同じ番号に設定）。

```
Manager A> CREATE ENCO KEY=1 TYPE=GENERAL
    VALUE="secret" ↵

Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル（.CFG）に、このコマンドを記述しても無効になります。
なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では、ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

25 接続相手との IKE ネゴシエーション要求を受け入れる ISAKMP ポリシー「i」を作成します。KEY には、前の手順で作成した事前共有鍵（鍵番号 1）を、PEER には拠点 B のルーターの IP アドレスを指定します。

```
Manager A> CREATE ISAKMP POLICY="i"
    PEER=12.34.56.78 KEY=1 SENDN=TRUE ↵

Info (1082003): Operation successful.
```

26 IPsec 通信の仕様を定義する SA スペック 1 を作成します。トンネルモード（デフォルト）、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager A> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
    PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↵

Info (1081003): Operation successful.
```

27 SA スペック 1だけからなる SA バンドルスペック 1 を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager A> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
    STRING="1" ↵

Info (1081003): Operation successful.
```

28 ISAKMP メッセージを素通しさせる IPsecポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの 500 番ポートからリモートの500 番ポート宛の UDP パケット(ISAKMP)に設定します。

```
Manager A> CREATE IPSEC POLICY="isa"
    INT=ppp0-1 ACTION=PERMIT LPORT=500
    RPORT=500 TRANSPORT=UDP ↵

Info (1081003): Operation successful.
```

ISAKMP を使用する場合は、必ず最初の IPsec ポリシーでISAKMPメッセージが通過できるような設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドのPOSITIONパラメーターを使用します。

29 実際の IPsec 通信に使用する IPsec ポリシー「vpn」を PPP0-1 に対して作成します。鍵管理方式「ISAKMP」、PEER には拠点B のルーターの IP アドレスを、BUNDLE には SA バンドルスペック「1」を指定します。

```
Manager A> CREATE IPSEC POLICY="vpn" INT=ppp0-
    1 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=12.34.56.78 ↵

Info (1081003): Operation successful.
```

30 IPsecポリシー「vpn」に対して実際に IPsec通信を行なう IP アドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

```
Manager A> SET IPSEC POLICY="vpn"
    LAD=192.168.1.0 LMA=255.255.255.0
    RAD=192.168.2.0 RMA=255.255.255.0 ↵

Info (1081003): Operation successful.
```

31 インターネットへの平文通信を許可する IPsec ポリシー「inet」をPPP0-1 に対して作成します。

```
Manager A> CREATE IPSEC POLICY="inet"
    INT=ppp0-1 ACTION=PERMIT ↵

Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後の IPsecポリシーで、すべてのパケットを通過させるための上記の設定を行ってください。どの IPsec ポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、設定がないとVPN以外との通信ができなくなります。

32 IPsecモジュールを有効にします。

```
Manager A> ENABLE IPSEC ↵

Info (1081003): Operation successful.
```

33 ISAKMP モジュールを有効にします。

```
Manager A> ENABLE ISAKMP ↵

Info (1082057): ISAKMP has been enabled.
```

34 Security Officer レベルのユーザーでログインしなおします。

```
Manager A> LOGIN secoff ↵

Password: passwdSA
```

35 動作モードをセキュリティーモードに切り替えます。

```
SecOff A> ENABLE SYSTEM SECURITY_MODE ↵

Info (1034003): Operation successful.
```

セキュリティーモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO(Remote Security Officer)の設定を行っておいてください。

本書「5.4 ノーマルモード / セキュリティーモード」(p.52)

●設定の保存

36 設定を保存します。

```
SecOff A> CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

37 保存したファイルを起動時設定ファイルに指定します。

```
SecOff A> SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

拠点Bの設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

3 管理をしやすくするために、本製品にシステム名を設定します。サイトBには「B」を設定します。

```
Manager > SET SYSTEM NAME=B ↵

Info (1034003): Operation successful.

Manager B>
```

4 IPsecはセキュリティーモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officerレベルのユーザーを登録しておきます。Security Officerのパスワードは厳重に管理してください。

ここでは、ユーザー名「secoff」、パスワード「passwdSB」を仮定します。

```
Manager B> ADD USER=secoff PASSWORD=passwdSB
    PRIVILEGE=SECURITYOFFICER ↵

User Authentication Database
------------------------------------------------------------------------------
Username: secoff ()
  Status: enabled    Privilege: Sec Off   Telnet: no     Login: yes
  Logins: 0          Fails: 0        Sent: 0            Rcvd: 0
  Authentications: 0 Fails: 0
------------------------------------------------------------------------------
```

●PPPの設定

5 WAN側Ethernetインターフェース（eth0）上にPPPインターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知されたPPPoEの「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager B> CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

6 プロバイダーから通知されたPPPユーザー名とパスワードを指定します。LQRはオフにし、代わりにLCP Echoパケットを使ってPPPリンクの状態を監視し、自動的にPPPoEのセッションを再接続するようにします（セッションキープアライブ）。また、ISDN向けの機能であるBAPはオフにします。

```
Manager B> SET PPP=0 OVER=eth0-any BAP=OFF
    USER=site_b@example.co.jp PASS-
    WORD=passwd_b LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

●IP、ルーティングの設定

7 IPモジュールを有効にします。

```
Manager B> ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

8 LAN側（vlan1）インターフェースにプライベートIPアドレスを割り当て、クライアント用のサブネットとします。

```
Manager B> ADD IP INT=vlan1 IP=192.168.2.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

9 WAN側（ppp0）インターフェースにプロバイダーから割り当てられたIPアドレスを設定します。

```
Manager B> ADD IP INT=ppp0 IP=12.34.56.78
    MASK=255.255.255.255 ↵

Info (1005275): interface successfully added.
```

10 デフォルトルートを設定します。

```
Manager B> ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

11 ファイアウォール機能を有効にします。

```
Manager B> ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

12 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager B> CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

13 ICMPパケットはPing（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*9

```
Manager B> ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

14 identプロキシー機能を無効にし、外部のメール（SMTP）サーバーなどからのident要求に対して、ただちにTCP RSTを返すよう設定します。

```
Manager B> DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

15 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN側（vlan1）インターフェースをPRIVATE（内部）に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

WAN側（ppp0）インターフェースをPUBLIC（外部）に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

16 LAN　側（vlan1）ネットワークに接続されているすべてのコンピューターがENAT機能を使用できるよう設定します。グローバルアドレスにはppp0のアドレスを使用します。

```
Manager B> ADD FIREWALL POLICY=net
    NAT=ENHANCED INT=vlan1 GBLINT=ppp0

Info (1077003): Operation successful.
```

17 接続相手からのIKEパケット（UDP500番）がファイアウォールを通過できるように設定します。

```
Manager B> ADD FIREWALL POLICY=net RU=1
    AC=ALLOW INT=ppp0 PROT=UDP GBLPO=500
    GBLIP=12.34.56.78 PO=500 IP=12.34.56.78 ↵

Info (1077003): Operation successful.
```

18 ローカルLANからリモートLANへのパケットにはNATをかけないように設定します。

```
Manager B> ADD FIREWALL POLICY=net RU=2
    AC=NONAT INT=vlan1 PROT=ALL
    IP=192.168.2.1-192.168.2.254 ↵

Info (1077003): Operation successful.

Manager B> SET FIREWALL POLICY=net RU=2
    REMOTEIP=192.168.1.1-192.168.1.254 ↵

Info (1077003): Operation successful.
```

19 基本ルールのままではIPsecパケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsecパケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点IPアドレスが192.168.2.1～192.168.2.254、つまりローカルLAN側ならば、NATの対象外とする」の意味になります。

```
Manager B> ADD FIREWALL POLICY=net RU=3
    AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-
    192.168.2.254 ENCAP=IPSEC ↵

Info (1077003): Operation successful.
```

*9 デフォルト設定では、ICMPはファイアウォールを通過できません。

●IPsec の設定

20 ここからが IPsec の設定になります。最初にISAKMP 用の事前共有鍵（pre-shared key）を作成します。拠点 A で指定した鍵番号を 1 番と、鍵の値「secret」を指定します。

```
Manager B> CREATE ENCO KEY=1 TYPE=GENERAL
    VALUE="secret" ↵

Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル（.CFG）に、このコマンドを記述しても無効になります。

なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では、ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

21 接続相手との IKE ネゴシエーション要求を受け入れる ISAKMP ポリシー「i」を作成します。KEY には、前の手順で作成した事前共有鍵（鍵番号 1）を、PEER には拠点 A のルーターの IP アドレスを指定します。

```
Manager B> CREATE ISAKMP POLICY="i"
    PEER=192.0.2.1 KEY=1 SENDN=TRUE ↵
```

22 IPsec 通信の仕様を定義する SA スペック 1 を作成します。拠点 A 同様にトンネルモード（デフォルト）、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager B> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
    PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↵

Info (1081003): Operation successful.
```

23 SA スペック 1だけからなる SA バンドルスペック 1 を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager B> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
    STRING="1" ↵

Info (1081003): Operation successful.
```

24 ISAKMP メッセージを素通しさせる IPsec ポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの 500 番ポートからリモートの 500番ポート宛の UDP パケット（ISAKMP）に設定します。

```
Manager B> CREATE IPSEC POLICY="isa"
    INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
    TRANSPORT=UDP ↵

Info (1081003): Operation successful.
```

ISAKMP を使用する場合は、必ず最初の IPsec ポリシーで ISAKMPメッセージが通過できるような設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドのPOSITIONパラメーターを使用します。

25 実際の IPsec 通信に使用する IPsec ポリシー「vpn」を PPP0 に対して作成します。鍵管理方式「ISAKMP」、PEER には拠点 A のルーターの IP アドレスを、BUNDLE には SA バンドルスペック「1」を指定します。

```
Manager B> CREATE IPSEC POLICY="vpn" INT=ppp0
    ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=192.0.2.1 ↵

Info (1081003): Operation successful.
```

26 IPsec ポリシー「vpn」に対して実際に IPsec 通信を行なう IP アドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

```
Manager B> SET IPSEC POLICY="vpn"
    LAD=192.168.2.0 LMA=255.255.255.0
    RAD=192.168.1.0 RMA=255.255.255.0 ↵

Info (1081003): Operation successful.
```

27 インターネットへの平文通信を許可する IPsec ポリシー「inet」を PPP インターフェース0 に対して作成します。

```
Manager B> CREATE IPSEC POLICY="inet"
    INT=ppp0 ACTION=PERMIT ↵

Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後の IPsec ポリシーですべてのパケットを通過させる設定を行ってください。どの IPsec ポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、上記の設定がないと VPN 以外との通信ができなくなります。

28 IPsecモジュールを有効にします。

```
Manager B> ENABLE IPSEC ↵

Info (1081003): Operation successful.
```

29 ISAKMP モジュールを有効にします。

```
Manager B> ENABLE ISAKMP ↵

Info (1082057): ISAKMP has been enabled.
```

30 Security Officer レベルのユーザーでログインしなおします。

```
Manager B> LOGIN secoff ↵

Password: passwdSB
```

31 動作モードをセキュリティーモードに切り替えます。

```
SecOff B> ENABLE SYSTEM SECURITY_MODE ↵

Info (1034003): Operation successful.
```

セキュリティーモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO(Remote Security Officer)の設定を行っておいてください。

本書「5.4 ノーマルモード / セキュリティーモード」(p.52)

●**設定の保存**

32 設定を保存します。

```
SecOff A> CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

33 保存したファイルを起動時設定ファイルに指定します。

```
SecOff A> SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

接続の確認

34「SHOW PPP」コマンドで PPP の接続が確立(OPENED)したことを確認してください。

35 LAN 側のコンピューターから、相手側の社内サーバーなどが参照できることを確認してください。*10

まとめ

拠点 A、B それぞれで、前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 13.6.4 設定スクリプトファイル 拠点A

1	SET SYSTEM NAME=A
2	ADD USER=secoff PASSWORD=passwdSA PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=eth1 IP=192.0.2.2 MASK=255.255.255.248
8	ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0
9	ADD IP INT=ppp0-0 IP=0.0.0.0
10	ADD IP INT=ppp0-1 IP=192.0.2.1 MASK=255.255.255.255
11	ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXTHOP=0.0.0.0
12	ENABLE FIREWALL
13	CREATE FIREWALL POLICY=net
14	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
15	DISABLE FIREWALL POLICY=net IDENTPROXY
16	ADD FIREWALL POLICY=net INT=eth1 TYPE=PRIVATE
17	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18	ADD FIREWALL POLICY=net INT=ppp0-0 TYPE=PUBLIC
19	ADD FIREWALL POLICY=net INT=ppp0-1 TYPE=PUBLIC
20	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0-1 GBLIP=192.0.2.1
21	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.3 PORT=80

*10 サブネット間でWindowsのネットワークドライブを参照するためには、例えばWindows 2000/XP では「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーの IP アドレスなどを指定します。
(例)¥¥192.168.1.10

表13.6.4 設定スクリプトファイル 拠点A（続き）

22	ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4 PORT=25
23	ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4 PORT=53
24	ADD FIREWALL POLICY=net RULE=4 AC=ALLOW INT=ppp0-1 PROTO=UDP IP=192.0.2.4 PORT=53
25	ADD FIREWALL POLICY=net RU=5 AC=ALLOW INT=ppp0-1 PROTO=UDP GBLPO=500 GBLIP=192.0.2.1 PO=500 IP=192.0.2.1
26	ADD FIREWALL POLICY=net RU=6 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1-192.168.1.254
27	SET FIREWALL POLICY=net RU=6 REMOTEIP=192.168.2.1-192.168.2.254
28	ADD FIREWALL POLICY=net RU=7 AC=NONAT INT=ppp0-1 PROT=ALL IP=192.168.1.1-192.168.1.254 ENCAP=IPSEC
29	CREATE ISAKMP POLICY="i" PEER=12.34.56.78 KEY=1 SENDN=TRUE
30	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
31	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
32	CREATE IPSEC POLICY="isa" INT=ppp0-1 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
33	CREATE IPSEC POLICY="vpn" INT=ppp0-1 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=12.34.56.78
34	SET IPSEC POLICY="vpn" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.2.0 RMA=255.255.255.0
35	CREATE IPSEC POLICY="inet" INT=ppp0-1 ACTION=PERMIT
36	ENABLE IPSEC
37	ENABLE ISAKMP

表13.6.5 設定スクリプトファイル 拠点B

1	SET SYSTEM NAME=B
2	ADD USER=secoff PASSWORD=passwdSB PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_b@example.co.jp PASSWORD=passwd_b LQR=OFF ECHO=ON
5	ENABLE IP
6	ADD IP INT=vlan1 IP=192.168.2.1 MASK=255.255.255.0
7	ADD IP INT=ppp0 IP=12.34.56.78 MASK=255.255.255.255

表13.6.5 設定スクリプトファイル 拠点B（続き）

8	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
9	ENABLE FIREWALL
10	CREATE FIREWALL POLICY=net
11	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
12	DISABLE FIREWALL POLICY=net IDENTPROXY
13	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
14	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
15	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
16	ADD FIREWALL POLICY=net RU=1 AC=ALLOW INT=ppp0 PROT=UDP GBLPO=500 GBLIP=12.34.56.78 PO=500 IP=12.34.56.78
17	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.2.1-192.168.2.254
18	SET FIREWALL POLICY=net RU=2 REMOTEIP=192.168.1.1-192.168.1.254
19	ADD FIREWALL POLICY=net RU=3 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-192.168.2.254 ENCAP=IPSEC
20	CREATE ISAKMP POLICY="i" PEER=192.0.2.1 KEY=1 SENDN=TRUE
21	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
22	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
23	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
24	CREATE IPSEC POLICY="vpn" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=192.0.2.1
25	SET IPSEC POLICY="vpn" LAD=192.168.2.0 LMA=255.255.255.0 RAD=192.168.1.0 RMA=255.255.255.0
26	CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT
27	ENABLE IPSEC
28	ENABLE ISAKMP

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

13.7 インターネット接続による３点間 IPsec VPN

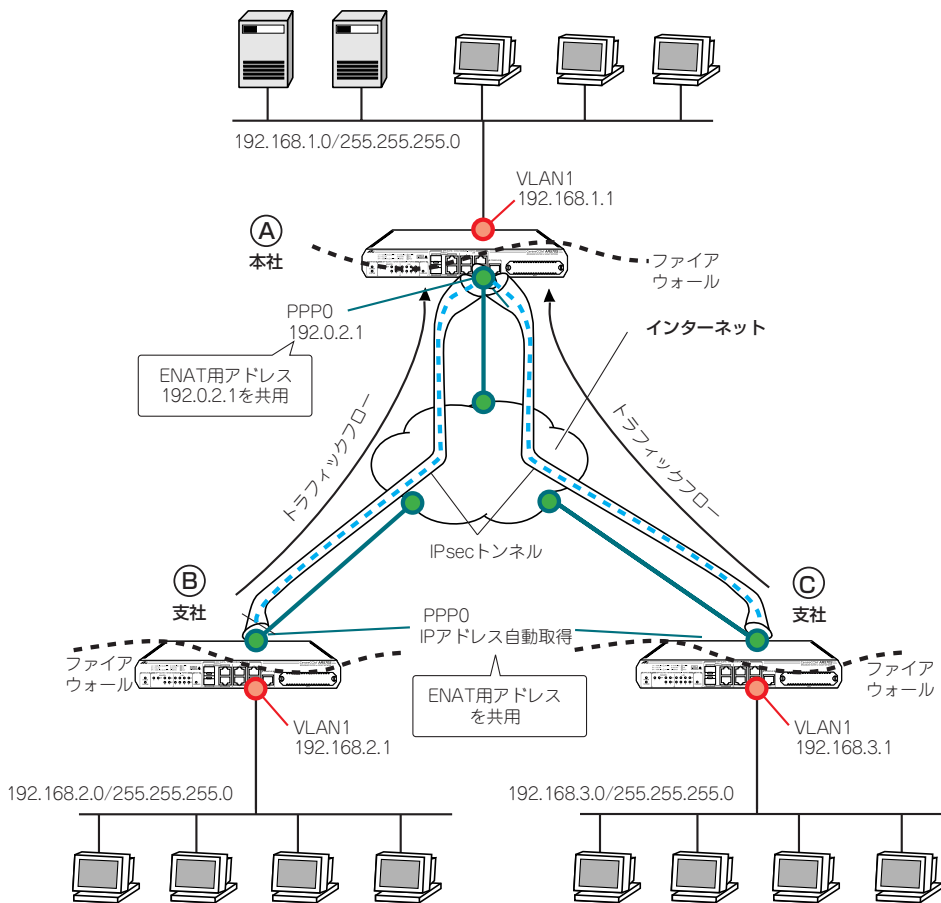



図 13.7.1 IPsec による接続

PPPoE でインターネットに接続している 3 つの拠点を、IPsec で接続しデータの安全性を確保します。

この例では、本社と各支社の接続を例にあげます。以下の 3 拠点間の接続を、トンネルモード（ESP）で暗号化します。ただし、本社支社間の安全な通信経路を確保することを目的とし、各支社間の通信は行いません。

- グローバルアドレス 1 個を固定的に割り当てられている拠点 A（本社）
- グローバルアドレス 1 個をに割り当てられている拠点 B、C（支社）

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●拠点 A

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：192.0.2.1/32（1 個固定）

- DNS サーバー：接続時に通知される

●拠点B

- 接続のユーザー名：site_b@example.co.jp
- 接続のパスワード：passwd_b
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：1 個不定
- DNS サーバー：接続時に通知される

●拠点C

- 接続のユーザー名：site_c@example.co.jp
- 接続のパスワード：passwd_c
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：1 個不定
- DNS サーバー：接続時に通知される

設定の方針

●インターネット接続設定

- すべての拠点においてグローバルアドレスの割り当ては 1 個しかないので、WAN 側（ppp0）インターフェースにグローバルアドレスを設定したダイナミック ENAT による、通常の端末型を使用します。このグローバルアドレスが IPsec パケットの始点アドレスとしてセットされます。

表 13.7.1 インターネット接続設定

	拠点 A	拠点 B	拠点 B
WAN 側物理インターフェース	eth0	eth0	eth0
WAN 側 IP アドレス（ppp0）	192.0.2.1/32	動的割り当て	動的割り当て
LAN 側 IP アドレス（vlan1）	192.168.1.1/24（vlan1）	192.168.2.1/24（vlan1）	192.168.3.1/24（vlan1）

●VPN設定

- IPsec トンネルは、拠点 A の ppp0 と拠点 B の ppp0 の間、拠点 A の ppp0 と拠点 C の ppp0 の間にそれぞれ別個に張られます。このトンネルはプライベートLAN 間を接続するためのもので、IP のパケットを暗号化して通します。

- ファイアウォールの設定においては、IPsec 関連のパケット（IKE、ESP）を除く外部からの不正アクセスを遮断し、内部からは自由にインターネットへのアクセスができるようにします。

- トンネリング対象のパケットにNAT が適用されないようルールを設定します。

表 13.7.2 IKE フェーズ 1（ISAKMP SA のネゴシエーション）

本製品間の認証方式	事前共有鍵（pre-shared key）
IKE 交換モード	Aggressive モード
事前共有鍵（A-B 間）	secret-ab（文字列）
事前共有鍵（A-C 間）	secret-ac（文字列）
拠点 A のルーターの認証 ID	IP アドレス :192.0.2.1（デフォルト）
拠点 B のルーターの認証 ID	名前 :client_B
拠点 C のルーターの認証 ID	名前 :client_C
Oakley グループ	1（デフォルト）
ISAKMP メッセージの暗号化方式	DES（デフォルト）
ISAKMP メッセージの認証方式	SHA1（デフォルト）
ISAKMP SA の有効期限（時間）	86400 秒（24 時間）（デフォルト）
ISAKMP SA の有効期限（Kbyte 数）	なし（デフォルト）
起動時のISAKMP ネゴシエーション	行わない

表 13.7.3 IKE フェーズ 2（IPsec SA のネゴシエーション）

SA モード	トンネルモード
セキュリティープロトコル	ESP（暗号＋認証）
暗号化方式	DES
認証方式	SHA1
IPComp	使わない
IPsec SA の有効期限（時間）	28800 秒（8 時間）（デフォルト）
IPsec SA の有効期限（Kbyte 数）	なし（デフォルト）
IPsec の適用対象 IP アドレス（A-B 間）	192.168.1.0/24 ⇔ 192.168.2.0/24
トンネル終端アドレス（A-B 間）	192.0.2.1 ⇔ 不定
IPsec の適用対象 IP アドレス（A-C 間）	192.168.1.0/24 ⇔ 192.168.3.0/24
トンネル終端アドレス（A-C 間）	192.0.2.1 ⇔ 不定
インターネットとの平文通信	行なう

拠点 A の設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

3 管理をしやすくするために、本製品にシステム名を設定します。サイト A には「A」を設定します。

```
Manager > SET SYSTEM NAME=A ↵

Info (1034003): Operation successful.

Manager A>
```

4 IPsecはセキュリティーモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officer レベルのユーザーを登録しておきます。Security Officer のパスワードは厳重に管理してください。

ここでは、ユーザー名「secoff」、パスワード「passwdSA」を仮定します。

```
Manager A> ADD USER=secoff PASSWORD=passwdSA
    PRIVILEGE=SECURITYOFFICER ↵

User Authentication Database
------------------------------------------------------------------------------
Username: secoff ()
   Status: enabled    Privilege: Sec Off   Telnet: no    Login: yes
   Logins: 0          Fails: 0       Sent: 0         Rcvd: 0
   Authentications: 0 Fails: 0
------------------------------------------------------------------------------
```

● PPP の設定

5 WAN 側 Ethernet インターフェース（eth0）上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager A> CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

6 プロバイダーから通知された PPP ユーザー名とパスワードを指定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視し、自動的に PPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

```
Manager A> SET PPP=0 OVER=eth0-any BAP=OFF
    USER=site_a@example.co.jp
    PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

● IP、ルーティングの設定

7 IP モジュールを有効にします。

```
Manager A> ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

8 LAN 側（vlan1）インターフェースにプライベート IP アドレスを割り当てます。

```
Manager A> ADD IP INT=vlan1 IP=192.168.1.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

9 WAN 側（ppp0）インターフェースにプロバイダーから割り当てられたIP アドレスを設定します。

```
Manager A> ADD IP INT=ppp0 IP=192.0.2.1
    MASK=255.255.255.255 ↵

Info (1005275): interface successfully added.
```

10 デフォルトルートを設定します。

```
Manager A> ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

11 ファイアウォール機能を有効にします。

```
Manager A> ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

12 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager A> CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

13 ICMP パケットは Ping（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*11

```
Manager A> ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACHABLE ↵

Info (1077003): Operation successful.
```

14 ident プロキシー機能を無効にし、外部のメール（SMTP）サーバーなどからのident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager A> DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

15 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側（vlan1）インターフェースを PRIVATE（内部）に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

WAN 側（ppp0）インターフェースを PUBLIC（外部）に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

16 LAN 側（vlan1）ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。グローバルアドレスには ppp0 のIP アドレスを使用します。

```
Manager A> ADD FIREWALL POLICY=net
    NAT=ENHANCED INT=vlan1 GBLINT=ppp0 ↵

Info (1077003): Operation successful.
```

17 接続相手からの IKE パケット（UDP500 番）がファイアウォールを通過できるように設定します。

```
Manager A> ADD FIREWALL POLICY=net RU=1
    AC=ALLOW INT=ppp0 PROTO=UDP GBLPO=500
    GBLIP=192.0.2.1 PO=500 IP=192.0.2.1 ↵

Info (1077003): Operation successful.
```

*11 デフォルト設定では、ICMP はファイアウォールを通過できません。

18 各拠点向けのパケットにはNATの対象にしないように設定します。

拠点B 向けのルールは以下のようにします。

```
Manager A> ADD FIREWALL POLICY=net RU=2
    AC=NONAT INT=vlan1 PROT=ALL
    IP=192.168.1.1-192.168.1.254 ↵

Info (1077003): Operation successful.

Manager A> SET FIREWALL POLICY=net RU=2
    REMOTEIP=192.168.2.1-192.168.2.254 ↵

Info (1077003): Operation successful.
```

拠点C 向けのルールは以下のようにします。

```
Manager A> ADD FIREWALL POLICY=net RU=3
    AC=NONAT INT=vlan1 PROT=ALL
    IP=192.168.1.1-192.168.1.254 ↵

Info (1077003): Operation successful.

Manager A> SET FIREWALL POLICY=net RU=3
    REMOTEIP=192.168.3.1-192.168.3.254 ↵

Info (1077003): Operation successful.
```

19 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点 IP アドレスが 192.168.1.1 ～ 192.168.1.254、つまり拠点A 向けならば、NAT の対象外とする」の意味になります。

```
Manager A> ADD FIREWALL POLICY=net RU=4
    AC=NONAT INT=ppp0 PROT=ALL IP=192.168.1.1-
    192.168.1.254 ENCAP=IPSEC ↵

Info (1077003): Operation successful.
```

● **IPsec の設定**

20 ここからがIPsec の設定になります。最初に ISAKMP 用の事前共有鍵（pre-shared key）を作成します。ここでは拠点 B 向けは鍵番号を「1」番、鍵の値は「secret-ab」とし、拠点 C 向けは「2」番と「secret-ac」とします（拠点 B、Cのルーターも同様に設定）。

```
Manager A> CREATE ENCO KEY=1 TYPE=GENERAL
    VALUE="secret-ab" ↵

Info (1073003): Operation successful.

Manager A> CREATE ENCO KEY=2 TYPE=GENERAL
    VALUE="secret-ac" ↵

Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル（.CFG）に、このコマンドを記述しても無効になります。

なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では、ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

21 接続相手との IKE ネゴシエーション要求を受け入れる ISAKMP ポリシーを作成します。この例では相手のアドレスが不定なため、拠点B、CともにPEERに「ANY」を、MODEに「AGGRESSIVE」を指定して Aggressive モードを使うよう設定します。
拠点 B 向けには、KEY に前の手順で作成した鍵番号「1」を、REMOTEID で認証 ID「client_B」を指定し、ポリシー「i_B」として作成します。
拠点 C 向けには、KEY に前の手順で作成した鍵番号「2」を REMOTEID で認証 ID「client_C」を指定しポリシー「i_C」として作成します。

```
Manager A> CREATE ISAKMP POLICY="i_B" PEER=ANY
    KEY=1 SENDN=TRUE REMOTEID="client_B"
    MODE=AGGRESSIVE HEARTBEATMODE=BOTH ↵

Info (1082003): Operation successful.

Manager A> CREATE ISAKMP POLICY="i_C" PEER=ANY
    KEY=2 SENDN=TRUE REMOTEID="client_C"
    MODE=AGGRESSIVE HEARTBEATMODE=BOTH ↵

Info (1082003): Operation successful.
```

22 IPsec 通信の仕様を定義する SA スペック 1 を作成します。トンネルモード(デフォルト)、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager A> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
    PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↵

Info (1081003): Operation successful.
```

23 SA スペック 1だけからなる SA バンドルスペック 1 を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager A> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
    STRING="1" ↵

Info (1081003): Operation successful.
```

24 ISAKMP メッセージを素通しさせる IPsec ポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの 500 番ポートからリモートの500 番ポート宛の UDP パケット(ISAKMP)に設定します。

```
Manager A> CREATE IPSEC POLICY="isa"  INT=ppp0
    ACTION=PERMIT LPORT=500 RPORT=500
    TRANSPORT=UDP ↵

Info (1081003): Operation successful.
```

ISAKMP を使用する場合は、必ず最初の IPsec ポリシーで ISAKMPメッセージが通過できるような設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドのPOSITION パラメーターを使用します。

25 実際の IPsec 通信に使用する IPsec ポリシーを PPP0 に対して作成します。相手の IP アドレスが不定なので、PEER に「DYNAMIC」を指定します。鍵管理方式は「ISAKMP」、BUNDLE にはSA バンドルスペック「1」を指定します。
拠点B と拠点 C 向けの違いはポリシー名のみです。

```
Manager A> CREATE IPSEC POLICY="vpn_B"
    INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUN-
    DLE=1 PEER=DYNAMIC ↵

Info (1081003): Operation successful.

Manager A> CREATE IPSEC POLICY="vpn_C"
    INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUN-
    DLE=1 PEER=DYNAMIC ↵

Info (1081003): Operation successful.
```

26 IPsec ポリシーに対して、それぞれの拠点向けに実際に IPsec 通信を行なう IP アドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

```
Manager A> SET IPSEC POLICY="vpn_B"
    LAD=192.168.1.0 LMA=255.255.255.0
    RAD=192.168.2.0 RMA=255.255.255.0 ↵

Info (1081003): Operation successful.

Manager A> SET IPSEC POLICY="vpn_C"
    LAD=192.168.1.0 LMA=255.255.255.0
    RAD=192.168.3.0 RMA=255.255.255.0 ↵

Info (1081003): Operation successful.
```

27 インターネットへの平文通信を許可する IPsec ポリシー「inet」を PPP0 に対して作成します。

```
Manager A> CREATE IPSEC POLICY="inet" INT=ppp0
    ACTION=PERMIT ↵

Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後の IPsec ポリシーで、すべてのパケットを通過させるための上記の設定を行ってください。どの IPsec ポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、設定がないと VPN 以外との通信ができなくなります。

28 IPsec モジュールを有効にします。

```
Manager A> ENABLE IPSEC ↵

Info (1081003): Operation successful.
```

29 ISAKMP モジュールを有効にします。

```
Manager A> ENABLE ISAKMP ↵

Info (1082057): ISAKMP has been enabled.
```

30 Security Officer レベルのユーザーでログインしなおします。

```
Manager A> LOGIN secoff ↵

Password: passwdSA
```

31 動作モードをセキュリティーモードに切り替えます。

```
SecOff A> ENABLE SYSTEM SECURITY_MODE ↵

Info (1034003): Operation successful.
```

セキュリティーモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO（Remote Security Officer）の設定を行っておいてください。

本書「5.4 ノーマルモード / セキュリティーモード」(p.52)

●設定の保存

32 設定を保存します。

```
SecOff A> CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

33 保存したファイルを起動時設定ファイルに指定します。

```
SecOff A> SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

拠点 B、拠点 C の設定

拠点 B と拠点 C では、それぞれの拠点ごとの設定値が異なるだけで、基本的な設定方法は同じです。

拠点 B と拠点 C で設定値が違う部分については、それぞれ向けの操作例などを明示します。それ以外の部分は両拠点について同様の設定を行ってください。

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

3 管理をしやすくするために、本製品にシステム名を設定します。サイトＢ には「B」を設定します。

拠点B

```
Manager > SET SYSTEM NAME=B ↵

Info (1034003): Operation successful.

Manager B>
```

拠点Ｃ には「C」を設定します。

拠点C

```
Manager > SET SYSTEM NAME=C ↵

Info (1034003): Operation successful.

Manager C>
```

4 IPsec はセキュリティーモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officer レベルのユーザーを登録しておきます。Security Officer のパスワードは厳重に管理してください。

拠点 B では、ユーザー名「secoff」、パスワード「passwdSB」を仮定します。

拠点B

```
Manager B> ADD USER=secoff PASSWORD=passwdSB
 PRIVILEGE=SECURITYOFFICER ↵

User Authentication Database
---------------------------------------------------------------------------
Username: secoff ()
   Status: enabled    Privilege: Sec Off   Telnet: no    Login: yes
   Logins: 0          Fails: 0       Sent: 0           Rcvd: 0
   Authentications: 0 Fails: 0
---------------------------------------------------------------------------
```

拠点Ｃ では、ユーザー名「secoff」、パスワード「passwordSC」を仮定します。

拠点C

```
Manager C> ADD USER=secoff PASSWORD=passwdSC
    PRIVILEGE=SECURITYOFFICER ↵

User Authentication Database
---------------------------------------------------------------------------
Username: secoff ()
   Status: enabled    Privilege: Sec Off   Telnet: no    Login: yes
   Logins: 0          Fails: 0       Sent: 0           Rcvd: 0
   Authentications: 0 Fails: 0
---------------------------------------------------------------------------
```

● PPP の設定

5 WAN 側 Ethernet インターフェース（eth0）上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager B> CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

6 プロバイダーから通知されたPPP ユーザー名とパスワードを各拠点ごとに指定し接続時に IP アドレス割り当てを行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使ってPPP リンクの状態を監視し､自動的にPPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

拠点B

```
Manager B> SET PPP=0 OVER=eth0-any BAP=OFF
    USER=site_b@example.co.jp PASS-
    WORD=passwd_b IPREQUESRT=ON LQR=OFF
    ECHO=ON ↵

Info (1003003): Operation successful.
```

拠点C

```
Manager C> SET PPP=0 OVER=eth0-any BAP=OFF
    USER=site_c@example.co.jp PASS-
    WORD=passwd_c IPREQUESRT=ON LQR=OFF
    ECHO=ON ↵

Info (1003003): Operation successful.
```

●IP、ルーティングの設定

7 IP モジュールを有効にします。

```
Manager B> ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

8 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するように設定します。

```
Manager B> ENABLE IP REMOTEASSIGN ↵

Info (1005287): IP module has been enabled.
```

9 LAN 側（vlan1）インターフェースに各拠点ごとのプライベート IP アドレスを割り当て、クライアント用のサブネットとします。

拠点B

```
Manager B> ADD IP INT=vlan1 IP=192.168.2.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

拠点C

```
Manager C> ADD IP INT=vlan1 IP=192.168.3.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

10 WAN 側（ppp0）インターフェースにプロバイダーから割り当てられた IP アドレスを設定します。

```
Manager B> ADD IP INT=ppp0 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

11 デフォルトルートを設定します。

```
Manager B> ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

12 ファイアウォール機能を有効にします。

```
Manager B> ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

13 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager B> CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

14 ICMP パケットは Ping（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*12

```
Manager B> ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACHABLE ↵

Info (1077003): Operation successful.
```

15 ident プロキシー機能を無効にし、外部のメール（SMTP）サーバーなどからの ident要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager B> DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

ヒント

*12 デフォルト設定では、ICMP はファイアウォールを通過できません。

16 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側（vlan1）インターフェースを PRIVATE（内部）に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

WAN 側（ppp0）インターフェースを PUBLIC（外部）に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

17 LAN　側（vlan1）ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。グローバルアドレスにはppp0 のアドレスを使用します。

```
Manager B> ADD FIREWALL POLICY=net
    NAT=ENHANCED INT=vlan1 GBLINT=ppp0

Info (1077003): Operation successful.
```

18 ローカルLAN からリモート LANへのパケットには NAT をかけないように設定します。

拠点B

```
Manager B> ADD FIREWALL POLICY=net RU=1
    AC=NONAT INT=vlan1 PROT=ALL
    IP=192.168.2.1-192.168.2.254 ↵

Info (1077003): Operation successful.

Manager B> SET FIREWALL POLICY=net RU=1
    REMOTEIP=192.168.1.1-192.168.1.254 ↵

Info (1077003): Operation successful.
```

拠点C

```
Manager C> ADD FIREWALL POLICY=net RU=1
    AC=NONAT INT=vlan1 PROT=ALL
    IP=192.168.3.1-192.168.3.254 ↵

Info (1077003): Operation successful.

Manager C> SET FIREWALL POLICY=net RU=1
    REMOTEIP=192.168.1.1-192.168.1.254 ↵

Info (1077003): Operation successful.
```

19 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点 IP アドレスがローカルLAN 側ならば、NAT の対象外とする」の意味になります。IP にはそれぞれの拠点の LAN 側 IP アドレスの範囲を指定します。

拠点 B

```
Manager B> ADD FIREWALL POLICY=net RU=2
    AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-
    192.168.2.254 ENCAP=IPSEC ↵

Info (1077003): Operation successful.
```

拠点C

```
Manager C> ADD FIREWALL POLICY=net RU=2
    AC=NONAT INT=ppp0 PROT=ALL IP=192.168.3.1-
    192.168.3.254 ENCAP=IPSEC ↵

Info (1077003): Operation successful.
```

● IPsec の設定

20 ここからがIPsec の設定になります。最初に ISAKMP 用の事前共有鍵（pre-shared key）を作成します。鍵番号と、それぞれの拠点に対して拠点A で指定した鍵の値を指定します。

```
Manager B> CREATE ENCO KEY=1 TYPE=GENERAL
    VALUE="secret-ab" ↵

Info (1073003): Operation successful.
```

拠点C

```
Manager C> CREATE ENCO KEY=1 TYPE=GENERAL
    VALUE="secret-ac" ↵

Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル（.CFG）に、このコマンドを記述しても無効になります。

なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では,ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

21 前手順で作成した鍵を使い、接続相手とのIKEネゴシエーション要求を受け入れるISAKMPポリシー「i_A」を作成します。PEERにはルーターAのIPアドレスを指定します。また、自分のアドレスが不定なため、LOCALIDで自分の認証IDを指定し、MODEは「AGGRESSIVE」でAggressiveモードを使うよう設定します。拠点BではLOCALIDは「client_B」を、拠点Cには「client_C」を指定します。

拠点B

```
Manager B> CREATE ISAKMP POLICY="i_A"
    PEER=192.0.2.1 KEY=1 SENDN=TRUE
    LOCALID="client_B" MODE=AGGRESSIVE HEART-
    BEATMODE=BOTH ↵
```

拠点C

```
Manager C> CREATE ISAKMP POLICY="i_A"
    PEER=192.0.2.1 KEY=1 SENDN=TRUE
    LOCALID="client_C" MODE=AGGRESSIVE HEART-
    BEATMODE=BOTH ↵
```

22 IPsec通信の仕様を定義するSAスペック1を作成します。拠点A同様にトンネルモード(デフォルト)、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager B> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
    PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↵

Info (1081003): Operation successful.
```

23 SAスペック1だけからなるSAバンドルスペック1を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager B> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
    STRING="1" ↵

Info (1081003): Operation successful.
```

24 ISAKMPメッセージを素通しさせるIPsecポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの500番ポートからリモートの500番ポート宛のUDPパケット(ISAKMP)に設定します。

```
Manager B> CREATE IPSEC POLICY="isa"
    INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
    TRANSPORT=UDP ↵

Info (1081003): Operation successful.
```

ISAKMPを使用する場合は、必ず最初のIPsecポリシーでISAKMPメッセージが通過できるような設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドのPOSITIONパラメーターを使用します。

25 実際のIPsec通信に使用するIPsecポリシー「vpn_A」をPPP0に対して作成します。鍵管理方式「ISAKMP」、PEERには拠点AのルーターのIPアドレスを、BUNDLEにはSAバンドルスペック「1」を指定します。

```
Manager B> CREATE IPSEC POLICY="vpn_A"
    INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUN-
    DLE=1 PEER=192.0.2.1 ↵

Info (1081003): Operation successful.
```

26 IPsecポリシー「vpn_A」に対して実際にIPsec通信を行なうIPアドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

拠点B

```
Manager B> SET IPSEC POLICY="vpn_A"
    LAD=192.168.2.0 LMA=255.255.255.0
    RAD=192.168.1.0 RMA=255.255.255.0 ↵

Info (1081003): Operation successful.
```

拠点C

```
Manager C> SET IPSEC POLICY="vpn_A"
    LAD=192.168.3.0 LMA=255.255.255.0
    RAD=192.168.1.0 RMA=255.255.255.0 ↵

Info (1081003): Operation successful.
```

27 インターネットへの平文通信を許可するIPsecポリシー「inet」をPPPインターフェース0に対して作成します。

```
Manager B> CREATE IPSEC POLICY="inet"
    INT=ppp0 ACTION=PERMIT ↵

Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後のIPsecポリシーですべてのパケットを通過させる設定を行ってください。どのIPsecポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、上記の設定がないとVPN以外との通信ができなくなります。

28 IPsecモジュールを有効にします。

```
Manager B> ENABLE IPSEC ↵

Info (1081003): Operation successful.
```

29 ISAKMP モジュールを有効にします。

```
Manager B> ENABLE ISAKMP ↵

Info (1082057): ISAKMP has been enabled.
```

30 Security Officer レベルのユーザーでログインしなおします。

拠点B

```
Manager B> LOGIN secoff ↵

Password: passwdSB
```

拠点C

```
Manager C> LOGIN secoff ↵

Password: passwdSC
```

31 動作モードをセキュリティーモードに切り替えます。

```
SecOff B> ENABLE SYSTEM SECURITY_MODE ↵

Info (1034003): Operation successful.
```

セキュリティーモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO（Remote Security Officer）の設定を行っておいてください。

本書「5.4 ノーマルモード／ セキュリティーモード」（p.52）

●設定の保存

32 設定を保存します。

```
SecOff B> CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

33 保存したファイルを起動時設定ファイルに指定します。

```
SecOff B> SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

接続の確認

34 拠点A、B、C ともにUTP ケーブルを接続し、「SHOW PPP」コマンドでPPP の接続が確立（OPENED）したことを確認してください。

35 LAN 側のコンピューターから、相手側の社内サーバーなどが参照できることを確認してください。*13

*13 サブネット間でWindowsのネットワークドライブを参照するためには、例えばWindows 2000/XP では「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーの IP アドレスなどを指定します。
（例）¥¥192.168.1.10

まとめ

サイトA、B、Cそれぞれで、前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表13.7.4 設定スクリプトファイル 拠点A

1	SET SYSTEM NAME=A
2	ADD USER=secoff PASSWORD=passwdSA PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
5	ENABLE IP
6	ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0
7	ADD IP INT=ppp0 IP=192.0.2.1 MASK=255.255.255.255
8	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
9	ENABLE FIREWALL
10	CREATE FIREWALL POLICY=net
11	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
12	DISABLE FIREWALL POLICY=net IDENTPROXY
13	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
14	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
15	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
16	ADD FIREWALL POLICY=net RU=1 AC=ALLOW INT=ppp0 PROTO=UDP GBLPO=500 GBLIP=192.0.2.1 PO=500 IP=192.0.2.1
17	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1-192.168.1.254
18	SET FIREWALL POLICY=net RU=2 REMOTEIP=192.168.2.1-192.168.2.254
19	ADD FIREWALL POLICY=net RU=3 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1-192.168.1.254
20	SET FIREWALL POLICY=net RU=3 REMOTEIP=192.168.3.1-192.168.3.254
21	ADD FIREWALL POLICY=net RU=4 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.1.1-192.168.1.254 ENCAP=IPSEC
22	CREATE ISAKMP POLICY="i_B" PEER=ANY KEY=1 SENDN=TRUE REMOTEID="client_B" MODE=AGGRESSIVE HEARTBEATMODE=BOTH

表13.7.4 設定スクリプトファイル 拠点A（続き）

23	CREATE ISAKMP POLICY="i_C" PEER=ANY KEY=2 SENDN=TRUE REMOTEID="client_C" MODE=AGGRESSIVE HEARTBEATMODE=BOTH
24	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
25	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
26	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
27	CREATE IPSEC POLICY="vpn_B" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=DYNAMIC
28	CREATE IPSEC POLICY="vpn_C" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=DYNAMIC
29	SET IPSEC POLICY="vpn_B" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.2.0 RMA=255.255.255.0
30	SET IPSEC POLICY="vpn_C" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.3.0 RMA=255.255.255.0
31	CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT
32	ENABLE IPSEC
33	ENABLE ISAKMP

表 13.7.5 設定スクリプトファイル 拠点B

1	SET SYSTEM NAME=B
2	ADD USER=secoff PASSWORD=passwdSB PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_b@example.co.jp PASSWORD=passwd_b LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.2.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
10	ENABLE FIREWALL
11	CREATE FIREWALL POLICY=net
12	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
13	DISABLE FIREWALL POLICY=net IDENTPROXY
14	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
15	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
16	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
17	ADD FIREWALL POLICY=net RU=1 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.2.1-192.168.2.254
18	SET FIREWALL POLICY=net RU=1 REMOTEIP=192.168.1.1-192.168.1.254
19	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-192.168.2.254 ENCAP=IPSEC
20	CREATE ISAKMP POLICY="i_A" PEER=192.0.2.1 KEY=1 SENDN=TRUE LOCALID="client_B" MODE=AGGRESSIVE HEARTBEATMODE=BOTH
21	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
22	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
23	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
24	CREATE IPSEC POLICY="vpn_A" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=192.0.2.1
25	SET IPSEC POLICY="vpn_A" LAD=192.168.2.0 LMA=255.255.255.0 RAD=192.168.1.0 RMA=255.255.255.0
26	CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT

表 13.7.5 設定スクリプトファイル 拠点B（続き）

27	ENABLE IPSEC
28	ENABLE ISAKMP

表13.7.6 設定スクリプトファイル 拠点C

1	SET SYSTEM NAME=C
2	ADD USER=secoff PASSWORD=passwdSC PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_c@example.co.jp PASSWORD=passwd_c IPREQUEST=ON LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.3.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
10	ENABLE FIREWALL
11	CREATE FIREWALL POLICY=net
12	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
13	DISABLE FIREWALL POLICY=net IDENTPROXY
14	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
15	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
16	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
17	ADD FIREWALL POLICY=net RU=1 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.3.1-192.168.3.254
18	SET FIREWALL POLICY=net RU=1 REMOTEIP=192.168.1.1-192.168.1.254
19	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.3.1-192.168.3.254 ENCAP=IPSEC
20	CREATE ISAKMP POLICY="i_A" PEER=192.0.2.1 KEY=1 SENDN=TRUE LOCALID="client_C" MODE=AGGRESSIVE HEARTBEATMODE=BOTH
21	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
22	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
23	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
25	CREATE IPSEC POLICY="vpn_A" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=192.0.2.1
26	SET IPSEC POLICY="vpn_A" LAD=192.168.3.0 LMA=255.255.255.0 RAD=192.168.1.0 RMA=255.255.255.0
27	CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT

表13.7.6 設定スクリプトファイル 拠点C（続き）

28	ENABLE IPSEC
29	ENABLE ISAKMP

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

13.8 インターネットと CUG サービスの同時接続 (端末型)

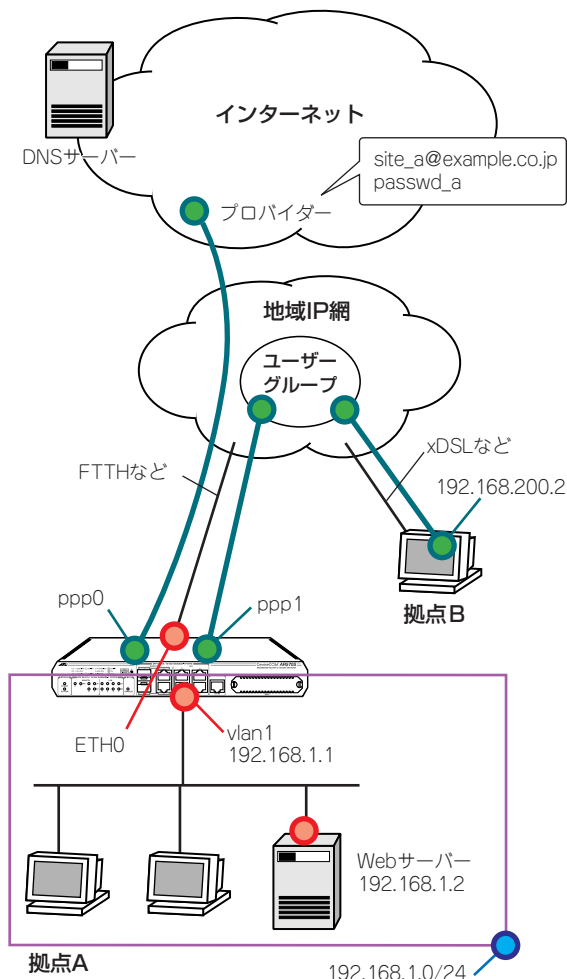



図13.8.1 インターネットとCUGサービスの同時接続(端末型)

PPPoE セッションを 2 本同時に使い、インターネット接続と、フレッツ・グループアクセス(ライト)およびフレッツ・グループ(ベーシックメニュー)の CUG(Closed Users Group)サービス(端末型)を同時に利用します。

この例では、LAN 側はプライベートアドレスで運用し、相手先のアドレスによって、スタティックな経路制御を行いパケットを振り分けます。クライアントはダイナミック ENAT 経由でインターネットや CUG サービスにアクセスします。また、ファイアウォールを使って外部からのアクセスを拒否します。

プロバイダーから提供される情報

以下の説明では、プロバイダーもしくはCUG サービスの管理者から下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●インターネット接続

- 接続のユーザー名:site_a@example.co.jp
- 接続のパスワード:passwd_a
- PPPoE サービス名:指定なし
- 使用できる IP アドレス:動的割り当て(1 個不定)
- DNS サーバー:接続時に通知される

● CUG サービス

- 接続のユーザー名:flets_a
- 接続のパスワード:fpasswd_a
- PPPoE サービス名:指定なし
- 使用できる IP アドレス:動的割り当て(1 個)
- 他のユーザーのIP アドレス:192.168.200.2/32

設定の方針

- スタティックルーティングにより、CUG サービス内の他ユーザー宛のパケットと、それ以外のパケット(インターネット宛て)の転送先を振り分けます。

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。

- ファイアウォールのダイナミック ENAT 機能を使用して、LAN 側ネットワークのプライベート IP アドレスを、WAN 側インターフェースに設定されたアドレスに変換します。インターネット宛てのパケットはプロバイダーから与えられたグローバル IP アドレスに、CUG サービス宛てのパケットは管理者から指定されたプライベート IP アドレスに変換します。これにより、LAN に接続された複数のコンピューターから、インターネット、CUG サービスへの同時アクセスが可能になります

- CUG サービスからのパケットは、ファイアウォールのルールを使用して、LAN 内の特定のサーバーに振り分けます。

  - Web サーバー(ポート80):192.168.1.2

- ルーターのDNS リレー機能をオンにして、LAN 側コンピューターからのDNS リクエストを、プロバイダーの DNS サーバーに転送します。

• 本製品の基本設定は、次の通りです。

表 13.8.1 本製品の基本設定

WAN 側物理インターフェース	eth0
インターネット向け WAN 側（ppp0）IP アドレス	不定
CUG サービス向け WAN 側（ppp1）IP アドレス	不定
LAN 側（vlan1）IP アドレス	192.168.1.1/32
DHCP サーバー機能	使わない

設定

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
 login: manager ↵
Password: friend（表示されません）
```

●PPP の設定

3 WAN 側 Ethernet インターフェース（eth0）上にインターネットと接続するための PPP インターフェース「0」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

4 プロバイダーから通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視し、自動的に PPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=site_a@example.co.jp
    PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

5 WAN 側 Ethernet インターフェース（eth0）上に CUG サービスと接続するための PPP インターフェース「1」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=1 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

6 CUG サービス管理者から通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視し、自動的に PPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=1 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=flets_a
    PASSWORD=fpasswd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

●IP、ルーティングの設定

7 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

8 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するように設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.
```

9 LAN 側（vlan1）インターフェースにプライベート IP アドレスを割り当て、クライアント用のサブネットとします。
CUG サービスのアドレス（ppp1）とは、重ならないものを指定してください。

```
Manager > ADD IP INT=vlan1 IP=192.168.1.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

10 インターネット接続用の WAN 側（ppp0）インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

11 CUG サービス接続用の WAN 側（ppp1）インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp1 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

12 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

13 CUG サービス向けの経路をスタティックに設定します。
CUG サービス内に複数の拠点がある場合には、それぞれの拠点ごとに経路を設定します。

```
Manager > ADD IP ROUTE=192.168.200.2
    MASK=255.255.255.255 INT=ppp1
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

14 DNS リレー機能を有効にします。

```
Manager > ENABLE IP DNSRELAY ↵

Info (1005003): Operation successful.
```

●ファイアウォールの設定

15 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

16 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

17 ICMP パケットは Ping（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*14

```
Manager > ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

18 ident プロキシー機能を無効にし、外部のメール（SMTP）サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager > DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

19 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側（vlan1）インターフェースを PRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

インターネット接続用の WAN 側（ppp0）インターフェースを PUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

*14 デフォルト設定では、ICMP はファイアウォールを通過できません。

CUG サービス接続用の WAN 側（ppp1）インターフェースをPUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp1
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

20 LAN 側ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。インターネット宛てパケットの場合は、NAT アドレスとして ppp0 の IP アドレスを使用します。CUG サービス宛てパケットの場合は、NAT アドレスとして ppp1 の IP アドレスを使用します。
ファイアウォールのダイナミック ENAT では、パケットが INT から GBLINT に転送されたときに、パケットの始点アドレスを GBLINT のアドレスに書き換えます。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=ppp0 ↵

Info (1077003): Operation successful.

Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=ppp1 ↵

Info (1077003): Operation successful.
```

21 CUG サービス側からのルーターに向けた HTTP（ポート 80）パケットを、LAN 内の IP アドレス 192.168.1.2 のサーバーに転送するルールを設定します。
他にも公開したいサーバーがあるときには、それぞれについて、ルールを設定します。
逆にサーバーを公開しない場合には、このルール設定は不要です。

```
Manager > ADD FIREWALL POLICY=net RU=1
    AC=ALLOW INT=ppp1 PROT=tcp PORT=80
    IP=192.168.1.2 GBLINT=0.0.0.0 GBLP=80 ↵

Info (1077003): Operation successful.
```

●時刻、パスワード、設定保存

22 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=01-APR-2005 ↵

System time is 01:00:01 on Sunday 01-APR-2005.
```

23 ユーザー「manager」のパスワードを変更します。Confirm：の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↵

Old password: friend ↵
New password: xxxxxxx ↵
Confirm: xxxxxxx ↵
```

24 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

25 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

●接続の確認

26 PPP の接続の確立は、「SHOW PPP」コマンドで確認できます。

```
Manager > SHOW PPP ↵

 Name          Enabled  ifIndex  Over                CP          State
 ------------------------------------------------------------------------
 ppp0            YES      04                         IPCP        OPENED
                                 eth0-any            LCP         OPENED
 ppp1            YES      04                         IPCP        OPENED
                                 eth0-any            LCP         OPENED
 ------------------------------------------------------------------------
```

27 LAN 側のコンピューターで Web ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。
なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合（DHCP クライアントである場合）、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

28 LAN 側のコンピューターから、CUG サービスで接続しているサーバーなどが参照できることを確認してください。*15

*15 サブネット間で Windows のネットワークドライブを参照するためには、例えば Windows 2000/XP では「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーの IP アドレスなどを指定します。
（例）¥¥192.168.1.10

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。。

表 13.8.2 設定スクリプトファイル（ROUTER.CFG）

1	CREATE PPP=0 OVER=eth0-any
2	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
3	CREATE PPP=1 OVER=eth0-any
4	SET PPP=1 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=flets_a PASSWORD=fpasswd_a LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP INT=ppp1 IP=0.0.0.0
10	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
11	ADD IP ROUTE=192.168.200.2 MASK=255.255.255.255 INT=ppp1 NEXTHOP=0.0.0.0
12	ENABLE IP DNSRELAY
13	ENABLE FIREWALL
14	CREATE FIREWALL POLICY=net
15	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
16	DISABLE FIREWALL POLICY=net IDENTPROXY
17	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
19	ADD FIREWALL POLICY=net INT=ppp1 TYPE=PUBLIC
20	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
21	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp1
22	ADD FIREWALL POLICY=net RU= 1 AC=ALLOW INT=ppp1 PROT=tcp PORT=80 IP=192.168.1.2 GBLIP=0.0.0.0 GBLP=80

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

13.9 インターネットと CUG サービスの同時接続（LAN 型）

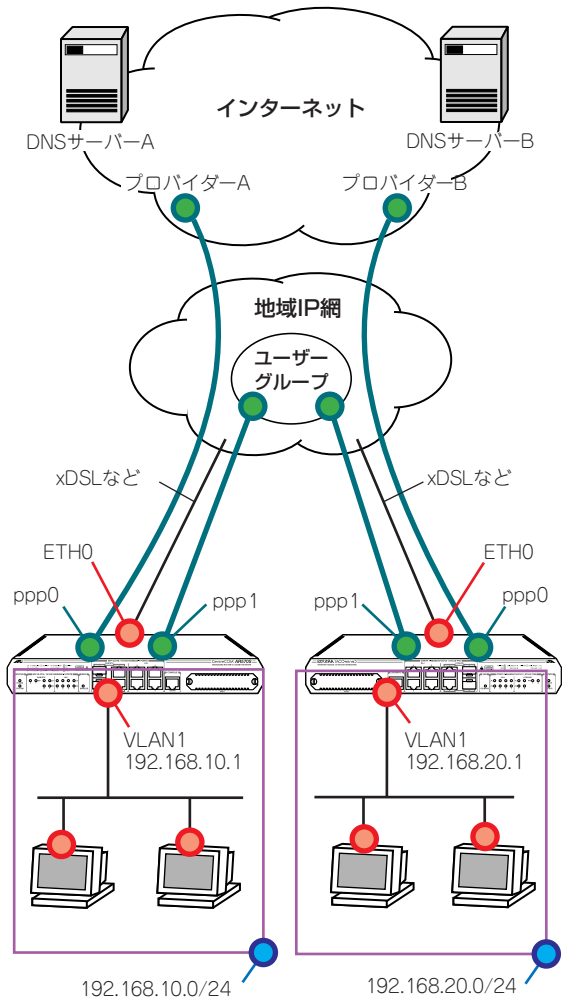



図 13.9.1 インターネットと CUG サービスの同時接続（LAN 型）

PPPoE セッションを 2 本同時に使って、インターネット接続と、フレッツ・グループアクセス（プロ）およびフレッツ・グループ（ビジネスメニュー）の CUG（Closed Users Group）サービス（LAN 型）を同時に利用します。

この例では、各拠点の LAN 側はプライベートアドレスで運用し、相手先のアドレスによって、スタティックな経路制御を行いパケットを

振り分けます。クライアントはインターネットにはダイナミックENAT経由で、CUGサービスにはプライベートアドレスのままでアクセスします。また、ファイアウォールを使って外部からのアクセスを拒否します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●拠点Aのインターネット接続

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoEサービス名：指定なし
- 使用できるIPアドレス：動的割り当て（1個不定）
- DNSサーバー：接続時に通知される

●拠点Bのインターネット接続

- 接続のユーザー名：site_b@example.co.jp
- 接続のパスワード：passwd_b
- PPPoEサービス名：指定なし
- 使用できるIPアドレス：動的割り当て（1個不定）
- DNSサーバー：接続時に通知される

●拠点AのCUGサービス

- 接続のユーザー名：flets_a
- 接続のパスワード：fpasswd_a
- PPPoEサービス名：指定なし
- CUGサービスのネットワークアドレス：192.168.10.0/24

●拠点BのCUGサービス

- 接続のユーザー名：flets_b
- 接続のパスワード：fpasswd_b
- PPPoEサービス名：指定なし
- CUGサービスのネットワークアドレス：192.168.20.0/24

設定の方針

- スタティックルーティングにより、CUGサービス内の他ユーザー宛のパケットと、それ以外のパケット（インターネット宛て）の転送先を振り分けます。

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。

- ファイアウォールのダイナミックENAT機能を使用して、インターネット宛てのパケットはLAN側ネットワークのプライベートIPアドレスを、インターネット向けWAN側インターフェースに設定されたアドレスに変換します。CUGサービス向けWAN側インターフェースはアンナンバードとして、LAN内のコンピューターは設定されたプライベートアドレスそのままで他の拠点にアクセスします。

- ルーターのDNSリレー機能をオンにして、LAN側コンピューターからのDNSリクエストを、プロバイダーのDNSサーバーに転送します。

- 本製品の基本設定は、次の通りです。

表 13.9.1 本製品の基本設定

WAN側物理インターフェース	eth0	eth0
インターネット向け WAN側（ppp0）IPアドレス	不定	不定
CUGサービス向け WAN側（ppp1）IPアドレス	不定	不定
LAN側（vlan1）IPアドレス	192.168.10.1 /24	192.168.20.1 /24
DHCPサーバー機能	使わない	使わない

設定

各拠点では、設定するIPアドレスなどの設定値が異なるだけで、基本的な設定方法は同じです。

各拠点で設定値が違う部分については、それぞれ向けの操作例などを明示します。それ以外の部分は両拠点について同様の設定を行ってください。

1 本製品の電源スイッチをオンにします。

2 コンソールポートから、ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager ↵
Password: friend（表示されません）
```

第2部 設定例編

● PPP の設定

3 WAN 側 Ethernet インターフェース（eth0）上にインターネットと接続するためのPPP インターフェース「0」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知されたPPPoEの「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

4 プロバイダーから通知されたPPP ユーザー名とパスワードをそれぞれの拠点ごとに指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視し、自動的に PPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

拠点A

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=site_a@example.co.jp
    PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

拠点B

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=site_b@example.co.jp
    PASSWORD=passwd_b LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

5 WAN 側 Ethernet インターフェース（eth0）上に CUG サービスと接続するための PPP インターフェース「1」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知されたPPPoEの「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=1 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

6 CUGサービス管理者から通知されたPPPユーザー名とパスワードをそれぞれの拠点ごとに指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使ってPPP リンクの状態を監視し、自動的にPPPoE のセッションを再接続するようにします（セッションキープアライブ）。また、ISDN 向けの機能である BAP はオフにします。

拠点A

```
Manager > SET PPP=1 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=flets_a
    PASSWORD=fpasswd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

拠点B

```
Manager > SET PPP=1 OVER=eth0-any BAP=OFF
    IPREQUEST=ON USER=flets_b
    PASSWORD=fpasswd_b LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

● IP、ルーティングの設定

7 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵

Info (1005287): IP module has been enabled.
```

8 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するように設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.
```

9 LAN 側（vlan1）インターフェースにCUG サービス管理者から指定されたIP アドレスをそれぞれの拠点ごとに指定します。

拠点A

```
Manager > ADD IP INT=vlan1 IP=192.168.10.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

拠点B

```
Manager > ADD IP INT=vlan1 IP=192.168.20.1
    MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.
```

10 インターネット接続用の WAN 側（ppp0）インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

11 CUG サービス接続用の WAN 側（ppp1）インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp1 IP=0.0.0.0 ↵

Info (1005275): interface successfully added.
```

12 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

13 他の拠点向けの経路をスタティックに設定します。拠点が 3 つ以上ある場合には、それぞれの拠点向けに ROUTE、MASK の値を適切なものに変更して、複数登録してください。

拠点A

```
Manager > ADD IP ROUTE=192.168.20.0
    MASK=255.255.255.0 INT=ppp1
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

拠点B

```
Manager > ADD IP ROUTE=192.168.10.0
    MASK=255.255.255.0 INT=ppp1
    NEXTHOP=0.0.0.0 ↵

Info (1005275): IP route successfully added.
```

14 DNS リレー機能を有効にします。

```
Manager > ENABLE IP DNSRELAY ↵

Info (1005003): Operation successful.
```

●ファイアウォールの設定

15 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↵

Info (1077257): 19-Apr-2002 19:55:22
  Firewall enabled.

Info (1077003): Operation successful.
```

16 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↵

Info (1077003): Operation successful.
```

17 ICMP パケットは Ping（Echo/Echo Reply）と到達不可能（Unreachable）のみ双方向で許可します。*16

```
Manager > ENABLE FIREWALL POLICY=net
    ICMP_F=PING,UNREACH ↵

Info (1077003): Operation successful.
```

18 ident プロキシー機能を無効にし、外部のメール（SMTP）サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager > DISABLE FIREWALL POLICY=net
    IDENTPROXY ↵

Info (1077003): Operation successful.
```

19 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側（vlan1）インターフェースを PRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

インターネット接続用の WAN 側（ppp0）インターフェースを PUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

*16 デフォルト設定では、ICMP はファイアウォールを通過できません。

CUG サービス接続用の WAN 側（ppp1）インターフェースをPUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp1
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

20 LAN 側ネットワークに接続されているすべてのコンピューターがインターネットへの通信にENAT 機能を使用できるよう設定します。NATアドレスとしてppp0のIPアドレスを使用します。ファイアウォールのダイナミックENAT では、パケットが INT から GBLINT に転送されたときに、パケットの始点アドレスをGBLINTのアドレスに書き換えます。
CUG サービス宛てパケットの場合は、NATは使いません。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=ppp0 ↵

Info (1077003): Operation successful.
```

21 他の拠点からの通信をすべて許可するルールを設定します。拠点が 3 つ以上ある場合には、すべての拠点の IP アドレスごとのREMOTEIP を指定したルールを設定してください。

拠点A

```
Manager > ADD FIREWALL POLICY=net RULE=1
    AC=ALLOW INT=ppp1 PROT=ALL
    REMOTEIP=192.168.20.1-192.168.20.254 ↵

Info (1077003): Operation successful.
```

拠点B

```
Manager > ADD FIREWALL POLICY=net RULE=1
    AC=ALLOW INT=ppp1 PROT=ALL
    REMOTEIP=192.168.10.1-192.168.10.254 ↵

Info (1077003): Operation successful.
```

●時刻、パスワード、設定保存

22 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=01-APR-2005 ↵

System time is 01:00:01 on Sunday 01-APR-2005.
```

23 ユーザー「manager」のパスワードを変更します。Confirm：の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↵

Old password: friend ↵
New password: xxxxxxx ↵
Confirm: xxxxxxx ↵
```

24 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

25 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

●接続の確認

26 PPP の接続の確立は、「SHOW PPP」コマンドで確認できます。

```
Manager > SHOW PPP ↵

 Name          Enabled  ifIndex  Over               CP          State
 ----------------------------------------------------------------------
 ppp0            YES      04                        IPCP        OPENED
                                 eth0-any           LCP         OPENED
 ppp1            YES      04                        IPCP        OPENED
                                 eth0-any           LCP         OPENED
 ----------------------------------------------------------------------
```

27 LAN 側のコンピューターでWeb ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。
なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合（DHCP クライアントである場合）、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

28 LAN 側のコンピューターから、CUG サービスで接続しているサーバーなどが参照できることを確認してください。[*17]

ヒント

*17 サブネット間でWindowsのネットワークドライブを参照するためには、例えばWindows 2000/XP では「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーの IP アドレスなどを指定します。
（例）¥¥192.168.1.10

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表13.9.2 拠点A の設定スクリプトファイル（ROUTERA.CFG）

1	CREATE PPP=0 OVER=eth0-any
2	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
3	CREATE PPP=1 OVER=eth0-any
4	SET PPP=1 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=flets_a PASSWORD=fpasswd_a LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.10.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP INT=ppp1 IP=0.0.0.0
10	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
11	ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INT=ppp1 NEXTHOP=0.0.0.0
12	ENABLE IP DNSRELAY
13	ENABLE FIREWALL
14	CREATE FIREWALL POLICY=net
15	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
16	DISABLE FIREWALL POLICY=net IDENTPROXY
17	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
19	ADD FIREWALL POLICY=net INT=ppp1 TYPE=PUBLIC
20	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
21	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp1 PROT=ALL REMOTEIP=192.168.20.1-192.168.20.254

表13.9.3 拠点B の設定スクリプトファイル（ROUTERB.CFG）

1	CREATE PPP=0 OVER=eth0-any
2	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_b@example.co.jp PASSWORD=passwd_b LQR=OFF ECHO=ON
3	CREATE PPP=1 OVER=eth0-any
4	SET PPP=1 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=flets_b PASSWORD=fpasswd_b LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP INT=ppp1 IP=0.0.0.0
10	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
11	ADD IP ROUTE=192.168.10.0 MASK=255.255.255.0 INT=ppp1 NEXTHOP=0.0.0.0
12	ENABLE IP DNSRELAY
13	ENABLE FIREWALL
14	CREATE FIREWALL POLICY=net
15	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
16	DISABLE FIREWALL POLICY=net IDENTPROXY
17	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
19	ADD FIREWALL POLICY=net INT=ppp1 TYPE=PUBLIC
20	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
21	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp1 PROT=ALL REMOTEIP=192.168.10.1-192.168.10.254

「SET TIME」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください

13.10 設定上の注意事項

PPPoE セッションの手動による切断

本設定では、本製品が起動すると同時に PPPoE セッションが確立され、以後常時接続された状態となります。PPPoE セッションの切断、再接続を行う場合は、手動で行います。

切断は、「DISABLE PPP」コマンドを実行します。

```
Manager > DISABLE PPP=0 ↵

Info (1003003): Operation successful.

Manager > SHOW PPP ↵

 Name          Enabled  ifIndex  Over                 CP          State
 --------------------------------------------------------------------------
 ppp0            NO       04                          IPCP        CLOSED
                                 eth0-any             LCP         INITIAL
 --------------------------------------------------------------------------
```

ただし、「DISABLE PPP」コマンドは、ランタイムメモリー上の PPP の設定スクリプトに追加されるので注意が必要です。
この状態で CREATE CONFIG コマンドを実行すると、
「disable ppp=0」は設定スクリプトファイルの内容として保存されます。本製品を再起動したとき、いつまで経っても PPP リンクが確立しません。

```
Manager > SHOW CONFIG DYN=PPP ↵

#
# PPP configuration
#
create ppp=0 over=eth0-any
set ppp=0 bap=off iprequest=on username="user1@isp" password="isppasswd1"
set ppp=0 over=eth0-any lqr=off echo=10
disable ppp=0
```

PPPoE セッションの再接続

「DISABLE PPP」コマンドによる切断を、再接続するには「RESTART ROUTER」コマンドを実行してください。

```
Manager > RESTART ROUTER ↵
```

PPPoE におけるアンナンバード

PPPoE の LAN 型接続では、IPCP ネゴシエーションによって、WAN 側（PPP）インターフェースにネットワークアドレス（ホスト部が 0 のアドレス）が割り当てられます。ネットワークアドレスは、ホストアドレスとしては使用できないため、事実上アンナンバードと同じですが、厳密に言うと専用線接続などで使用するアンナンバードとは異なります。

ルーター自身が WAN 側インターフェースから IP パケットを送出する場合を考えてみましょう。純粋なアンナンバードでは、送出インターフェースにアドレスが設定されていないため、他のインターフェースのアドレスを使用します。しかしながら、PPPoE LAN 型の場合は、まがりなりにも WAN 側インターフェースにアドレスが設定されているため、パケットの始点アドレスとして本来使用できないネットワークアドレスが使用されてしまいます（相手からの応答のパケットが届きません）。

通常は、ルーター自身がパケットを送信することはないため、このことを意識する必要はありませんが、L2TP、IPsec では注意が必要です。これらでカプセル化されたパケットには、始点アドレスとしてルーターの WAN 側インターフェースのアドレスが使用されるため、そのアドレスとして有効なものを使用しなければなりません。

有効なアドレスが使用されるようにするには、WAN 側インターフェースをマルチホーミングし、一方に有効なアドレスを設定した上で、デフォルトルートを有効なアドレスのインターフェースに向けてやります。

例えば、プロバイダーから 192.0.2.0/29 のアドレスが割り当てられているとすると、次のように設定します。この例では、LAN 側から WAN 側へのパケットは ppp0-1 にルーティングされ、始点アドレスとして 192.0.2.1 が使用されるようになります。

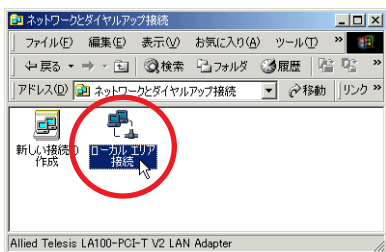
```
ADD IP INT=ppp0-0 IP=0.0.0.0
ADD IP INT=ppp0-1 IP=192.0.2.1
   MASK=255.255.255.255
ADD IP INT=VLAN1 IP=192.0.2.2
   MASK=255.255.255.248
ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXT=0.0.0.0
```

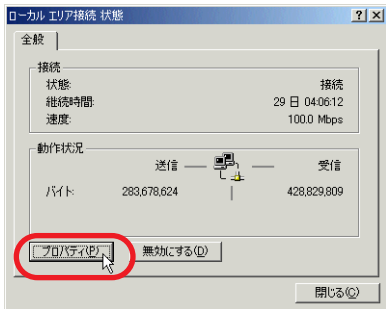
付録

A.1 コンピューターの設定

第2部「13 構成例」(p.75) のLAN 環境におけるコンピューター側の設定として、Windows 2000、Mac OS X の例を挙げます。Windows の他のバージョン、Mac OS の他のバージョンでは手順が異なりますが、以下の例を参考にして設定してください。

Windows 2000

1「コントロールパネル」→「ネットワークとダイヤルアップ接続」→「ローカルエリア接続」をダブルクリックしてください。

図A.1.1 「ローカルエリア接続」アイコン

2「プロパティ」をクリックしてください。

図A.1.2 ローカルエリア接続状態

3「インターネットプロトコル (TCP/IP)」を選択し、「プロパティ」をクリックしてください。

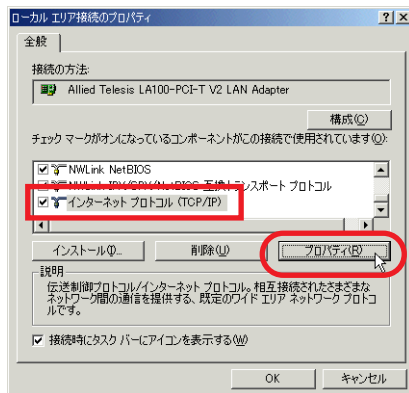



図 A.1.3 ローカルエリア接続のプロパティ

4 本製品（DHCP サーバー）からIP アドレスを自動的に取得する場合は、次のように設定してください（この設定は、Windows 2000におけるデフォルトです）。「IP アドレスを自動的に取得する」と「DNS サーバーの IP アドレスを自動的に取得する」をクリックし、「OK」をクリックしてください。

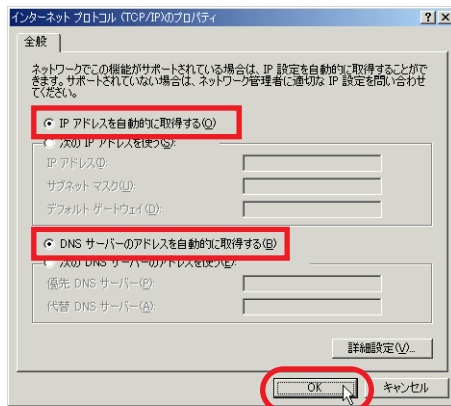



図 A.1.4 IP アドレス自動取得（DHCP クライアント）

付録

IP アドレスなどを固定的に設定する場合は、次のように設定してください。「次の IP アドレスを使う」をクリックし、「IP アドレス」「サブネットマスク」「デフォルトゲートウェイ」を入力します。「デフォルトゲートウェイ」は、本製品の LAN 側の IP アドレスを指定します。さらに、「次の DNS サーバーの IP アドレスを使う」をクリックし、「優先 DNS サーバー」に本製品の LAN 側の IP アドレスを入力します（本製品に DNS リレーの設定が必要です）。「代替 DNS サーバー」は空欄のままにしておきます。最後に、「OK」をクリックしてください。

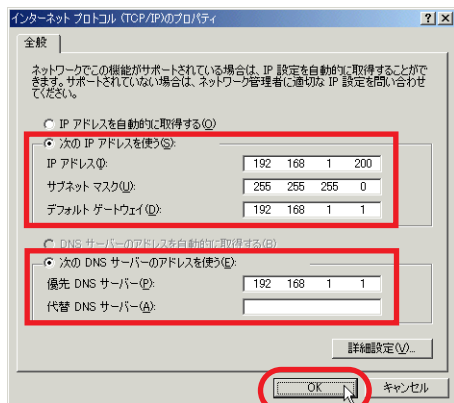



図 A.1.5 IP アドレス固定（DNS リレー）

DNS リレーを使用しない場合は、プロバイダーの DNS サーバーを直接指定します。

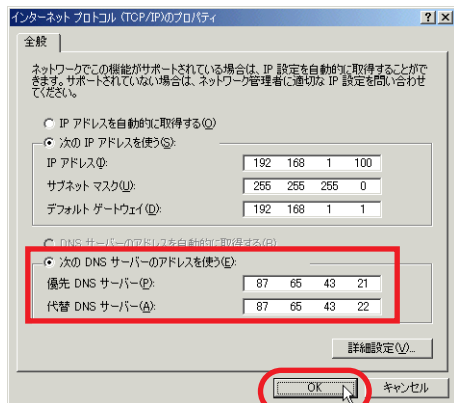



図 A.1.6 IP アドレス固定（DNS ダイレクト）

5 再起動を促すダイアログが現れたら、指示に従い再起動してください。

Mac OS X

1 「アップルメニュー」→「システム環境設定」を開いてください。

2 「システム環境設定」ダイアログボックスの「ネットワーク」をクリックしてください。

3 本製品（DHCP サーバー）から IP アドレスを自動的に取得する場合は、次のように設定してください（この設定は、Mac OS X におけるデフォルトです）。「表示」で「内蔵 Ethernet」を選択しておき、「TCP/IP」タブの「設定」で「DHCP サーバを参照」を選択します。最後に「今すぐ適用」をクリックしてください。本製品からの IP アドレス取得に成功すると、取得した IP アドレスなどの情報が表示されます（点線の囲み）。

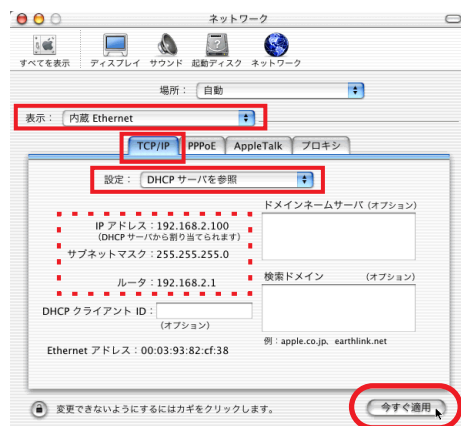



図 A.1.7 IP アドレス自動取得（DHCP クライアント）

IP アドレスなどを固定的に設定する場合は、次のように設定してください。「表示」で「内蔵 Ethernet」を選択しておき、「TCP/IP」タブの「設定」で「手入力」を選択します。「IP アドレス」「サブネットマスク」「ルータ」を入力します。「ルータ」は、本製品のLAN側のIP アドレスを指定します。「ドメインネームサーバ」に本製品の LAN 側の IP アドレスを入力します（本製品に DNS リレーの設定が必要です）。最後に、「今すぐ適用」をクリックしてください。

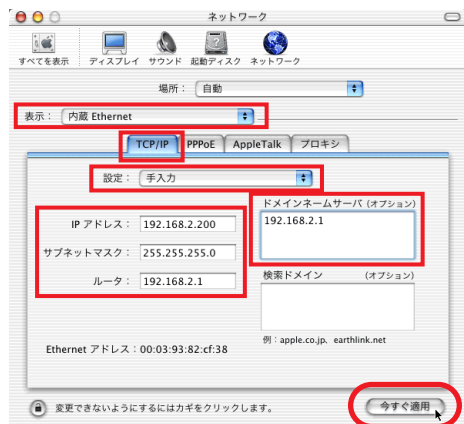



図 A.1.8 IP アドレス固定（DNS リレー）

DNS リレーを使用しない場合は、プロバイダーの DNS サーバーを直接指定します。

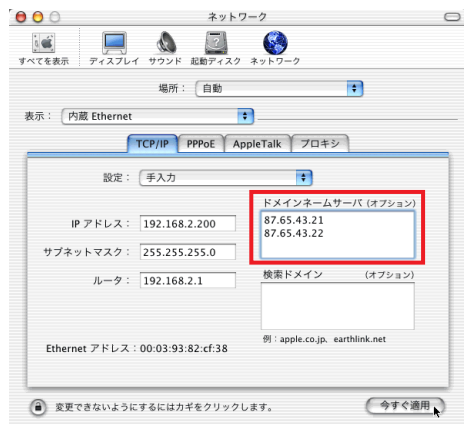



図 A.1.9 IP アドレス固定（DNS ダイレクト）

4 「ネットワーク」ダイアログボックスを閉じてください。

A.2 Microsoft Telnet の設定

Telnet クライアントとして、Windows XP、2000 に付属のものを使用する例を示します。Windows の他のバージョンの Telnet や、他の Telnet クライアントをご使用の場合は、手順が異なりますが、以下の例を参考にして設定してください。

Telnet クライアントに設定するパラメーターは、下記の通りです。エミュレーション、「BackSpace」キーのコードは EDIT コマンドのための設定です。文字セットは、HELP コマンド（日本語オンラインヘルプ）のための設定です。

表 1.2.1 Telnet クライアントの設定

項目	値
エミュレーション	VT100
「BackSpace」キーのコード	Delete
文字セット	SJIS

1 「スタート」ボタンをクリックし、「ファイル名を指定して実行」をクリックしてください。ダイアログボックスが現れますので、「名前」ボックスに「telnet」と入力して「OK」ボタンをクリックしてください。

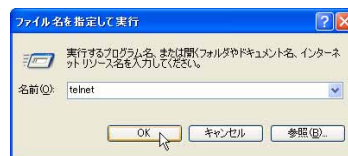



図 A.2.1 telnet の起動

2 Telnet が起動しプロンプトが表示されますので、次の 3 つのコマンドを入力してください。

```
Microsoft Telnet> set term vt100 ↵
Microsoft Telnet> set bsasdel ↵
Microsoft Telnet> set codeset Shift JIS ↵
```

「display」で設定状態を確認できます。

```
Microsoft Telnet> display ↵
```

3 Telnet を終了してください。次回の Telnet の起動には、上記の設定が適用されます。

```
Microsoft Telnet> quit ↵
```

A.3 ハイパーターミナルの設定

コンソールターミナルとして、Windows 2000、XP のハイパーターミナルを使用する例を示します。Windows の他のバージョンのハイパーターミナルや、他の通信ソフトウェアをご使用の場合は、手順が異なりますが、以下の例を参考にして設定してください。

通信ソフトウェアに設定するパラメーターは、下記の通りです。エミュレーション、「BackSpace」キーのコードは「EDIT」コマンドのための設定です。文字セットは、「HELP」コマンド（日本語オンラインヘルプ）のための設定です。

表 A.3.1 コンソールターミナルの設定

項目	値
インターフェース速度	9,600bps
データビット	8
パリティ	なし
ストップビット	1
フロー制御	ハードウェア（RTS/CTS）
エミュレーション	VT100
BackSpace キーのコード	Delete
エンコード	SJIS

1 「コンソールターミナルの接続」（p.23）に従い、本製品背面の CONSOLE ポートとコンピューター（Windows 2000）を接続してください。

2 Windows 2000 を起動し、「スタート」→「プログラム」→「アクセサリ」→「通信」→「ハイパーターミナル」をクリックしてください。

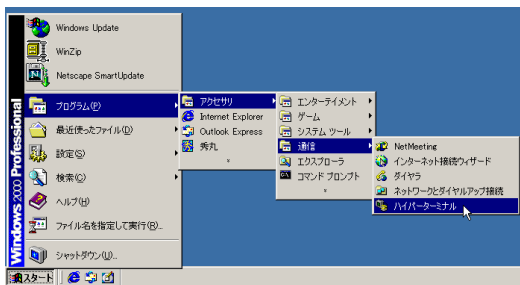



図 A.3.1 「ハイパーターミナル」フォルダ

3 次のダイアログボックスが現れたら[*1]、「国名 / 地域名」で「日本」を選択、「市外局番 / エリアコード」を入力して「OK」をクリックしてください。ここでは市外局番として「03」、外線発信番号は「無し」（0 発信しない）、ダイヤル方法は「トーン」を仮定しています。

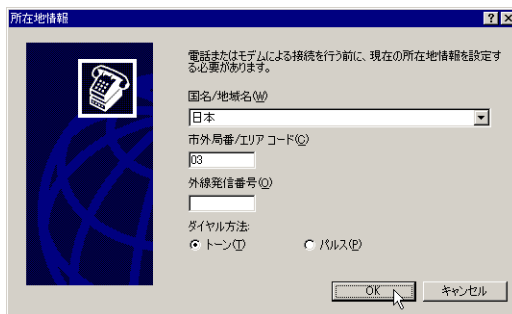



図 A.3.2 「所在地情報」の設定

4 次のダイアログボックスが現れたら、「OK」をクリックしてください。

図 A.3.3 「電話とモデムのオプション」の設定

5 接続の「名前」を入力、「アイコン」を選択して「OK」をクリックしてください。ここでは「名前」として「AR_ROUTER」を仮定しています。

*1 電話とモデムの設定が完了している場合、図 A.3.2、図 A.3.3 のダイアログボックスは表示されません。

図 A.3.4 接続の名前を入力

6「接続の方法」を選択し、「OK」をクリックしてください。ここではコンピューターの COM1 ポートにコンソールケーブルを接続すると仮定し、「COM1」を選択しています。他のポートに接続している場合は、接続しているポートを指定してください。

図 A.3.5 接続方法で COM1 を指定

7「ビット / 秒」で「9600」、「データビット」で「8」、「パリティ」で「なし」、「ストップビット」で「1」、「フロー制御」で「ハードウェア」を選択し、「OK」をクリックしてください（「ビット / 秒」以外はデフォルトです）。

図 A.3.6 「COM1」のプロパティの設定

8 ハイパーターミナルの画面が表示されます。

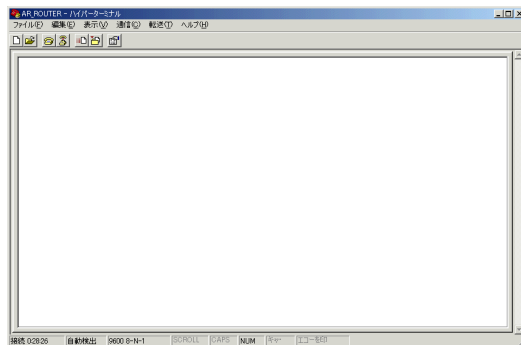



図 A.3.7 ターミナル画面

9「ファイル」→「プロパティ」をクリックしてください。「AR_ROUTER のプロパティ」ダイアログボックスが現れます。「設定」ページを選択し、「エミュレーション」で「VT100J」、「BackSpace キーの送信方法」で「Delete」を選択してください。「エンコード方法」をクリックしてください。

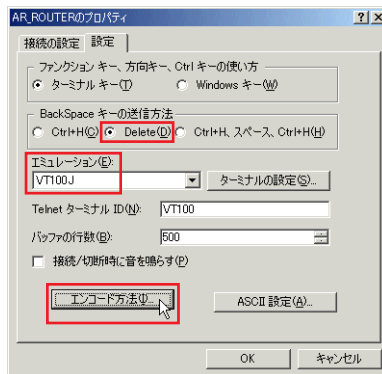



図 A.3.8 キーの設定

10「Shift-JIS」を選択し、「OK」をクリックしてください。下記のダイアログボックスが閉じ、図 A.3.8 に戻りますので、「OK」をクリックしてください。

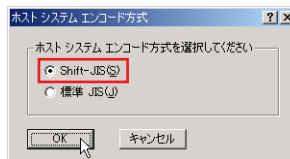



図 A.3.9 エンコード方式

11 以上で、ハイパーターミナルをコンソールターミナルとして使用するための設定は終了です。

ハイパーターミナルの設定の保存

次回のハイパーターミナルの実行の便宜のために、前述の手順で施した内容を保存しておきます。

1「ファイル」→「名前を付けて保存」をクリックしてください。

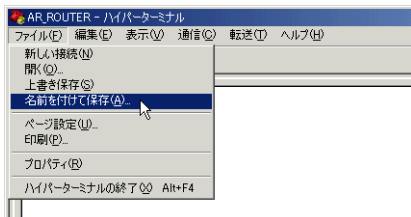



図 A.3.10 ハイパーターミナル設定の保存

2「ファイル名」に「A.3 ハイパーターミナルの設定」の手順 5 で指定した名前のファイル（拡張子は ht）が表示されていることを確認し、「保存」をクリックしてください。

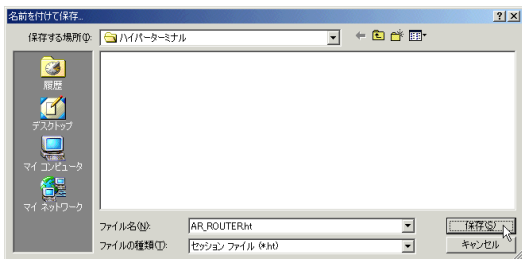



図 A.3.11 ハイパーターミナル設定ファイル名の入力

次回のハイパーターミナルの起動は、「スタート」→「プログラム」→「アクセサリ」→「通信」→「ハイパーターミナル」フォルダー→「AR_ROUTER.ht」をクリックしてください。

ハイパーターミナルの終了

1 本製品にログインしている場合は、ログアウトしてください。

2「ファイル」→「ハイパーターミナルの終了」をクリックしてください。

3 次のメッセージボックスが現れたら、「OK」をクリックしてください。

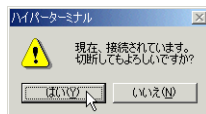



図 A.3.12 接続中の警告

A.4 CONSOLE ポート

本製品の CONSOLE ポートは、RJ-45 コネクターが使用されています。下記に結線表を示します。ピン番号は図 A.5.1 をご覧ください。

表 A.4.1 結線表

RS-232DCE	信号名（JIS 規格）	信号内容
1	RTS（RS）	送信要求
2	DTR（ER）	データ端末レディ
3	TXD（SD）	送信データ
4	GND（SG）	信号用接地
5	GND（SG）	信号用接地
6	RXD（RD）	受信データ
7	DSR（DR）	データセットレディ
8	CTS（CS）	送信可

コンソールターミナル（コンピューター、DTE）との接続は、別売の下記ケーブルをご使用ください。

- CentreCOM VT-Kit2：RJ-45/D-Sub 9 ピン（メス）変換ケーブル
- CentreCOM VT-Kit2 plus：RJ-45/USB または RJ-45/D-Sub 9 ピン（メス）変換ケーブル

A.5 10BASE-T/100BASE-TX/ 1000BASE-T インターフェース

本製品は、LAN 側として 4 つの、WAN 側または DMZ 用として 2 つの 10BASE-T/100BASE-TX/1000BASE-T インターフェースを持っています。各ポートは、RJ-45 型と呼ばれるモジュラージャックが使用されています。

これらのポートは、常に MDI/MDI-X 自動切替になっているため、どのポートもカスケードポートとして使用できます。また、ストレート、クロスケーブルのどちらを使用しても、正常に動作します。

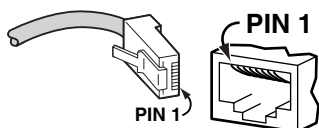



図 A.5.1 RJ-45 モジュラープラグ（左）、ジャック（右）

信号線名は下記の通りです。

表 A.5.1 信号線名

ピン番号	1000BASE-T		10BASE-T/100BASE-TX	
	MDI	MDI-X	MDI	MDI-X
1	BI_DA+	BI_DB+	TD+（送信）	RD+（受信）
2	BI_DA-	BI_DB-	TD-（送信）	RD-（受信）
3	BI_DB+	BI_DA+	RD+（受信）	TD+（送信）
4	BI_DC+	BI_DD+	未使用	未使用
5	BI_DC-	BI_DD-	未使用	未使用
6	BI_DB-	BI_DA-	RD-（受信）	TD-（送信）
7	BI_DD+	BI_DC+	未使用	未使用
8	BI_DD-	BI_DC-	未使用	未使用

ケーブルの結線は下記の通りです。

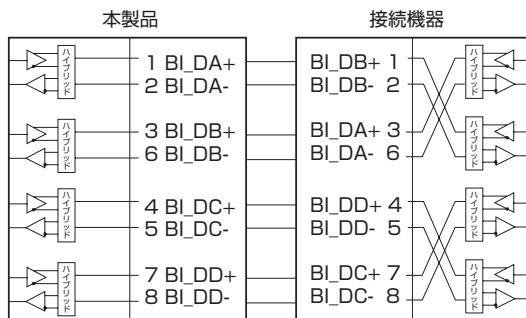



図 1.5.2 1000BASE-T ケーブル結線図

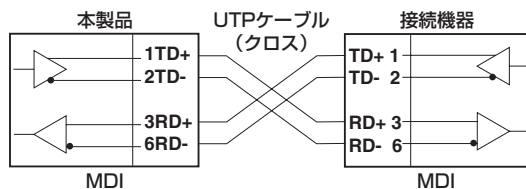
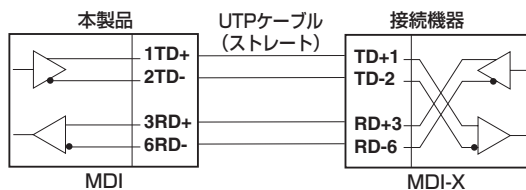
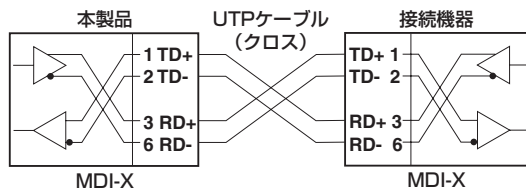
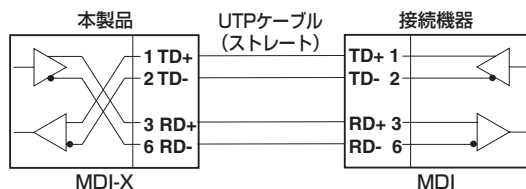



図 1.5.3 10BASE-T/100BASE-TX ケーブル結線図

A.6 PIC（Port Interface Card）

PIC（Port Interface Card）は、弊社 AR シリーズルーターの PIC ベイに装着して使用する拡張カードです。本製品は、次の 2 種類の PIC をサポートしています。

- AR020（PRI）
- AR021 V2（BRI）

PIC の取り付け

稲妻が発生しているときは、本製品の設置や、ケーブルの配線などの作業を行わないでください。落雷により感電する恐れがあります。

1 電源スイッチをオフにしてください。安全のために、コンセントから電源ケーブルを抜いてください。

PIC を本製品に取り付けるときは、必ず本製品の電源スイッチをオフにし、コンセントから電源ケーブルを抜いてください。電源が供給されたまま、この作業を行うと本製品や PIC の故障の原因となります。

2 PIC ブランクパネルを取り外してください。

3 PIC が AR021 V2（BRI）である場合は、必要に応じて基板上のジャンパーを設定してください。

PIC は静電気に敏感な部品を使用しています。部品が静電破壊する恐れがありますので、PIC の接点、部品などに素手で触れないでください。確実のためには、リストストラップなどの静電気防止用具の着用をお勧めします。

4 PIC を本製品の PIC ベイに取り付けます。PIC ベイのレールに PIC を沿わせ、カチンとショックがあるまで押し込んでください。

5 PIC の固定ネジ（2 本）を締めてください。

6 PIC のポートにケーブルを接続してください。

7 本製品の電源スイッチをオンにし、「SHOW SYSTEM」コマンドを入力して PIC が認識されていることを確認してください。下記に、AR020 の表示例を示します。

```
Manager > SHOW SYSTEM ↵

Router System Status                          Time 01:36:14 Date 05-Apr-2006.
Board      ID Bay  Board Name               Host Id Rev  Serial number
--------------------------------------------------------------------------------
Base       257     AR570S                      0 M2-0   D1656101A
PIC         75  0  AT-AR020-00 PIC E1/T1 PRI   0 M2-0   50087737
--------------------------------------------------------------------------------
Memory -   DRAM :131072 kB    FLASH : 32768 kB
Chip Revisions -
--------------------------------------------------------------------------------
......
```

PIC の取り外し

稲妻が発生しているときは、本製品の設置や、ケーブルの配線などの作業を行わないでください。落雷により感電する恐れがあります。

1 電源スイッチをオフにしてください。安全のために、コンセントから電源ケーブルを抜いてください。

PIC を本製品から取り外すときは、必ず本製品の電源スイッチをオフにし、コンセントから電源ケーブルを抜いてください。電源が供給されたまま、この作業を行うと本製品や PIC の故障の原因となります。

2 PIC のポートに接続されているケーブルを外してください。

3 PIC の固定ネジ（2 本）を締め、固定ネジを両手で持ちながら、手前に引き抜いてください。

PIC は静電気に敏感な部品を使用しています。部品が静電破壊する恐れがありますので、PIC の接点、部品などに素手で触れないでください。確実のためには、リストストラップなどの静電気防止用具の着用をお勧めします。

4 PIC ブランクパネルを取り付けてください。

AR020（PRI）

AR020 カードは、PRI ポート（G.703/Primary Rate ISDN WAN ポート）を 1 つ持つ PIC です。ISDN（23B+D）、192K 〜 1.5Mbps のデジタル専用線やフレームリレー網といったより高速なWAN回線への接続に使用します。

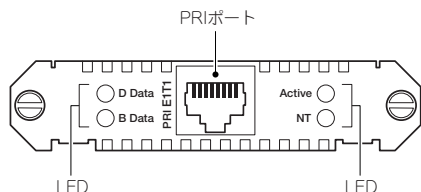



図 A.6.1 AR020背面パネル

PRI ポート

ISDN 回線またはデジタル専用線に接続するためのポートです。コネクターはRJ-45ジャックが使用されており、結線はIS10173に準拠しています。

LED

LED	色	状態	表示の内容
D Data	緑	点滅	本製品とISDN 交換機の間で、Dチャネルを経由してパケットが交換されています。ISDN においてのみ意味を持ちます。
		消灯	本製品とISDN 交換機の間で、Dチャネルを経由してパケットが交換されていません。
B Data	緑	点滅	本製品ともう一方の接続端の機器（通常はルーター）間で、任意のB チャネルを経由してパケットが交換されています。
		消灯	本製品ともう一方の接続端の機器（通常はルーター）間で、任意のB チャネルを経由してパケットが交換されていません。
Active	緑	点灯	レイヤ 1 のリンクが確立しています（本製品と交換機との間における通信が可能です）。
		消灯	レイヤ 1 のリンクが確立していません（本製品と交換機との間における通信ができません）。
NT	緑	点灯	PRI が ISDN NT モードで動作しています。 ISDN においてのみ意味を持ちます。
		消灯	PRI が ISDN TE モード（通常の動作モード）で動作しています。ISDN においてのみ意味を持ちます。

ジャンパー

ハードウェア Rev. の違いにより、3 ジャンパー型、2 ジャンパー型の 2 種類が存在します。ジャンパーは、ISDN、デジタル専用線、フレームリレー網の如何に関わらず、日本国内では常にデフォルト設定でご使用ください（3 ジャンパー型では J3：あり、J2：あり、J1：なし。2 ジャンパー型では J2：あり、J1：なし）。

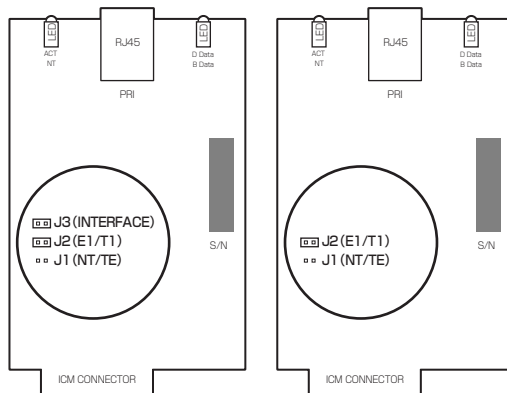



図 A.6.2 デフォルトのジャンパー設定

J1

ISDN の NT モード（本製品を交換機として網に接続）、または TE モード（本製品を端末として網に接続）を選択します。常に TE モードに設定してください（本製品は NT モードをサポートしておりません）。

J2

E1（Euro ISDN）または T1 を選択します。日本国内では T1 のみが使用可能です。

J3

E1 または T1（J2）に応じて、終端抵抗の値を選択します。日本国内では「あり」のみが可能です。2 ジャンパー型では、常に「J3：あり」となっています。

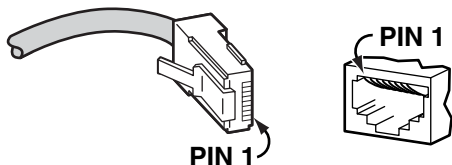
表 A.6.1 モードの設定

	あり	なし
J1	ISDN NT モード	**ISDN TE モード**
J2	**T1 モード**	E1 モード
J3	終端抵抗値を選択	

表A.6.2 終端抵抗値の設定

<table>
<tr><td>J2</td><td colspan="2">**あり（T1）**</td><td colspan="2">なし（E1）</td></tr>
<tr><td>J3</td><td>なし</td><td>**あり**</td><td>なし</td><td>あり</td></tr>
<tr><td>終端抵抗値</td><td>組み合わせ不可</td><td>**100Ω**</td><td>75Ω</td><td>120Ω</td></tr>
</table>

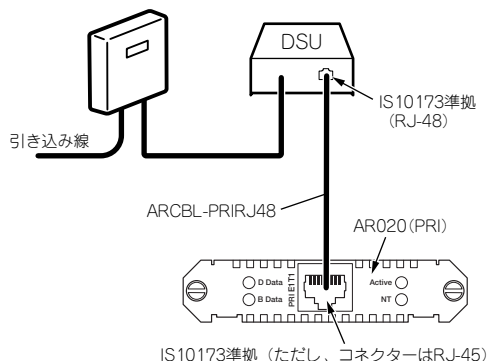
接続ケーブル

AR020のコネクターはRJ-45ジャックが使用されており､結線はIS10173に準拠しています。また、DSUはIS10173準拠、IS8877準拠の2種類が存在します。IS10173はPRIのための規格として最近規定されたもので､IS10173が規定される前は､PRIにおいてもBRIの規格であるIS8877が使用されていました。IS10173準拠のDSUはRJ-48ジャック（図A.6.3）を装備し、IS8877準拠のDSUはRJ-45ジャック（図A.5.1）を装備しています。IS10173規格とIS8877規格は、コネクター形状だけでなく結線も異なっています。

図A.6.3 RJ-48モジュラープラグ（左）、ジャック（右）

AR020には、DSUに接続するための、次の2種類のケーブルが付属しています。各ケーブルは、DSUの仕様に合わせてご使用ください（各ケーブルは、AR020専用です。他の用途に転用しないでください）。

- ARCBL-PRIRJ48
- ARCBL-PRIRJ45（IS10173-IS8877変換ケーブル）

ARCBL-PRIRJ48

AR020をIS10173に準拠したDSU（RJ-48ジャック）に接続する場合は､「ARCBL-PRIRJ48」をご使用ください。ARCBL-PRIRJ48は、一方がRJ-48、もう一方がRJ-45となっています。RJ-48のジャックとプラグには、誤挿入防止の凹凸があり、RJ-48のジャックとプラグ同士だけが嵌合可能です。

図A.6.4 IS10173準拠のDSUを使う場合

AR020（TE側、IS10173）			DSU（NT側、IS10173）	
機能	**ピン番号**		**ピン番号**	**機能**（注1）
受信＋	1	←	1	送信＋(RA)
受信－	2	←	2	送信－(RB)
---	3		3	---
送信＋	4	→	4	受信＋(TA)
送信－	5	→	5	受信－(TB)
---	6		6	---
---	7		7	---
---	8		8	---

注1 RA、RB、TA、TBは、DSUのネジ止め端子台の信号線名です。

図A.6.5 ARCBL-PRIRJ48による接続

ARCBL-PRIRJ45

AR020をIS8877に準拠したDSU（RJ-45ジャック）に接続する場合は､「ARCBL-PRIRJ45」をご使用ください。ARCBL-PRIRJ45の両端には、接続されるべき機器の種類が明記されており、RJ-45プラグの接続機器を入れ替えてご使用になることはできません。

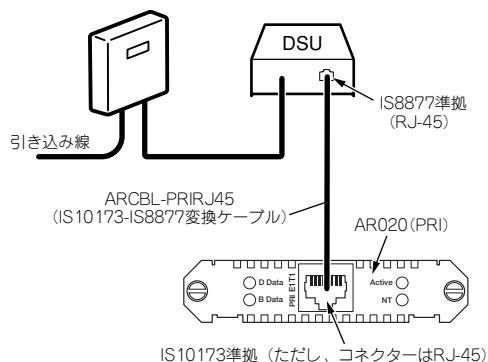



図 A.6.6 IS8877 準拠の DSU を使う場合

AR020（TE側、IS10173）	
機能	**ピン番号**
受信＋	1
受信−	2
---	3
送信＋	4
送信−	5
---	6
---	7
---	8

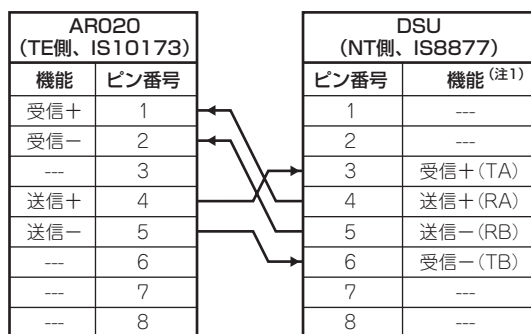
DSU（NT側、IS8877）	
ピン番号	**機能**（注1）
1	---
2	---
3	受信＋（TA）
4	送信＋（RA）
5	送信−（RB）
6	受信−（TB）
7	---
8	---

注1 RA、RB、TA、TBは、DSUのネジ止め端子台の信号線名です。

図 A.6.7 ARCBL-PRIRJ45 による接続

AR021 V2（BRI）

AR021 V2 カードは、BRI ポート（Basic Rate ISDN S/T WAN ポート、RJ-45）を 1 つ持つ PIC です。本製品を ISDN（2B+D）、64K〜128Kbps のデジタル専用線やフレームリレー網への接続に使用します。

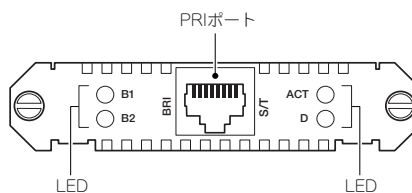



図 A.6.8 AR021 V2 背面パネル

BRI ポート

ISDN 回線またはデジタル専用線に接続するためのポートです。BRI ポートは、RJ-45 モジュラージャックが使用されており、結線は IS8877 に準拠しています。接続用ケーブルは別途ご用意ください。

表 A.6.3 BRI ポート結線

ピン番号	機能
1	---
2	---
3	送信 +
4	受信 +
5	受信 -
6	送信 -
7	---
8	---

LED

LED	色	状態	表示の内容
B1	緑	点灯	ISDN の B1 チャネルがもう一方の接続端の機器と接続しています。
		点滅	データの送受信が行われています。
		消灯	ISDN の B1 チャネルがもう一方の接続端の機器と接続していません。64Kbps または 128Kbps 専用線の場合は、通常消灯しています。

付録

B2	緑	点灯	ISDN の B2 チャネルがもう一方の接続端の機器と接続しています。
		点滅	データの送受信が行われています。ただし、64Kbps 専用線の場合は点滅しません。
		消灯	ISDN の B2 チャネルがもう一方の接続端の機器と接続していません。64Kbps または 128Kbps 専用線の場合は、通常消灯しています。
ACT	緑	点灯	レイヤ 1 のリンクが確立しています（本製品と交換機間の通信が可能です）。
		消灯	レイヤ 1 のリンクが確立していません（本製品と交換機間の通信ができません）。
D	緑	点滅	本製品と ISDN 交換機の間で、D チャネルを経由してパケットが交換されています。ISDN においてのみ意味を持ちます。
		消灯	本製品と ISDN 交換機の間で、D チャネルを経由してパケットが交換されていません。

ジャンパー

ジャンパー J1、J2 によって、終端抵抗（100Ω）のオン / オフを設定します。J1 は TX 線の終端、J2 は RX 線の終端です。終端抵抗は、2 つを揃えてオンまたはオフに設定しなければなりません（一方がオン、もう一方がオフは許されません）。デフォルトは「オン」です。

終端抵抗をオフにする場合、ジャンパープラグをジャンパーピンの一方にだけ挿してください（ジャンパープラグの紛失を防ぐことができます）。

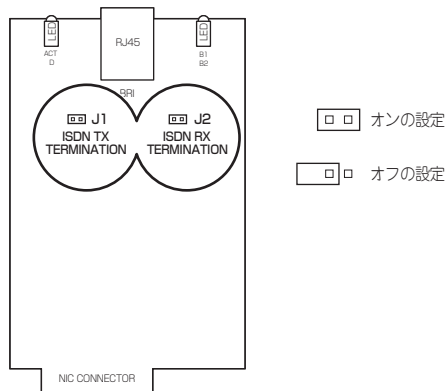



図 A.6.9 デフォルトのジャンパー設定

配線

回線 への接続にローゼット*2 が介在する場合、AR021 V2 の終端抵抗はオフ*3 に設定してください（J1：オフ、J2：オフ）。AR021 V2 を DSU に直結する場合、終端抵抗はオンに設定してください（J1：オン、J2：オン）。接続用ケーブルは、別途ご用意ください。

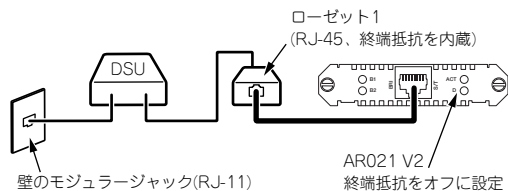



図 A.6.10 ローゼット 1 つの場合

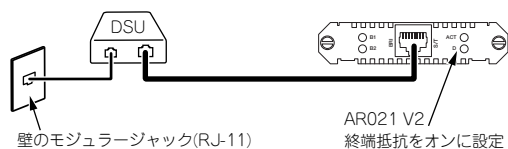



図 A.6.11 DSU に直結の場合

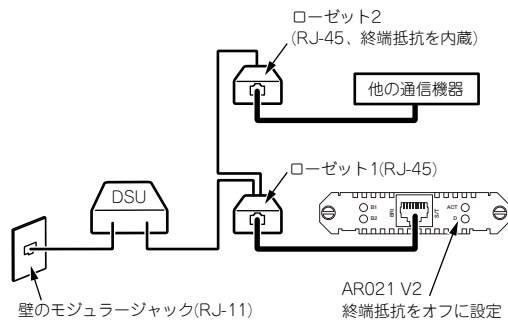



図 A.6.12 ローゼット 2 つの場合

*2 NS64 の場合、複数のローゼットの接続が可能です。デジタル専用線の場合、ローゼット 1 個の接続、または直結が可能です。回線のお申し込みの際にご確認ください。

*3 DSU から見て一番遠いローゼットには、終端抵抗が内蔵されているため、AR021 V2 の終端抵抗はオフに設定する必要があります。

A.7 製品仕様

ハードウェア

CPU	
PowerPC 833MHz	
メモリー容量	
メインメモリー	
128MByte	
フラッシュメモリー	
32MByte	
NVS	
512KByte	
インターフェース	
WAN ポート	
10BASE-T/100BASE-TX/1000BASE-T × 2[a] （オートネゴシエーション、Full Duplex/Half Duplex[b] / 10Mbps/100Mbps/1000Mbps 手動設定、常に MDI/MDI-X 自動切替） SFP スロット× 2	
LAN ポート	
10BASE-T/100BASE-TX/1000BASE-T × 4 （オートネゴシエーション、Full Duplex/Half Duplex[c] / 10Mbps/100Mbps/1000Mbps 手動設定、常に MDI/MDI-X 自動切替）	
コンソールポート	
RS-232（RJ-45 コネクター）× 1	
PIC ベイ× 1	
スイッチ部（LAN）	
スイッチング方式	
ストア＆フォワード	
パケットバッファー	
256KByte	
MAC アドレス登録数	
8K（最大）	
エージングタイム（MAC アドレス保持時間）	
約 300 秒	
電源部	
定格入力電圧	AC100-240V
	同梱の電源ケーブルは AC100V 用です。AC200V でご使用の場合は、設置業者にご相談ください。
入力電圧範囲	AC90-255V
定格周波数	50/60Hz
定格入力電流	2.1A
最大入力電流（実測値）	0.74A
平均消費電力	33W（最大 41W）
平均発熱量	120kJ/h（最大 150kJ/h）
環境条件	
動作時温度	0 ℃～ 50 ℃
動作時湿度	80％以下（結露なきこと）
保管時温度	－ 20 ℃～ 60 ℃
保管時湿度	95％以下（結露なきこと）
外形寸法	
305（W）× 232（D）× 44（H）mm（突起部含まず）	
質量	
2.3kg	
適合規格	
安全規格	UL60950-1 CSA-C 22.2 No.60950-1
EMI 規格	VCCI クラス A
電気通信事業法に基づく技術基準 JATE	
	CD05-0339001、L05-0011
準拠規格	
IEEE 802.3 10BASE-T	
IEEE 802.3u 100BASE-TX	
IEEE 802.3ab 1000BASE-T	
IEEE 802.3x Flow Control	
IEEE 802.1Q VLAN tagging	
IEEE 802.1p Class of Service	

a. 10BASE-T/100BASE-TX/1000BASE-T ポートと、SFP スロットはコンボポートです。
b. 1000BASE-T は Full Duplex のみです。
c. 1000BASE-T は Full Duplex のみです。

付録

ソフトウェア

このソフトウェア仕様は、ファームウェア Ver.2.7.5.B-03 の機能をもとに記載されています。機能は、ファームウェアのバージョンに依存します。ご使用になるファームウェアの機能は、最新のカタログ、リリースノートをご覧ください。

ルーティング対象プロトコル
IPv4、IPv6
ルーティング方式
RIP/RIP2、OSPF、BGP-4[a]、スタティック
WAN サービス
ADSL、CATV、FTTH、インターネット VPN、IP-VPN、広域イーサネットなどの各種ブロードバンド回線／サービス
ISDN、専用線、フレームリレー
機能
ファイアウォール（ステートフルインスペクション、攻撃検出・通知、アクセスリスト、アプリケーションゲートウェイ（SMTP プロキシー[b]、HTTP プロキシー[c]））
IP フィルター、経路制御フィルター
VPN（IPsec（DES、3DES/AES、ISAKMP/IKE、ISAKMP ハートビート、UDP ハートビート、ESP over UDP、NAT-Traversal、PKI[d]）、L2TP（LNS、ダイナミック L2TP）、GRE）
サービス管理（QoS（クラスベース）、Priority-Based ルーティング、Policy-based ルーティング、RSVP）
WAN ロードバランス機能[e]
NAT/EnhancedNAT、VRRP、UPnP、マルチホーミング、トリガー、ping ポーリング、DHCP（サーバー、クライアント、リレーエージェント）、DNS（リレー、キャッシュ、セレクション）
ブリッジング
タグ VLAN（IEEE 802.1Q）、ポートベース VLAN
データ圧縮（Stac LZS、Predictor、VJ Compression、FRF.9）
PAP/CHAP、RADIUS
PPPoE クライアント[f]、PPPoE セッションキープアライブ
PPP マルチリンク、PPP コールバック、PPP テンプレート（IP アドレスプール）
ISDN コールバック
管理機能
コマンドラインインターフェース
テキストエディター、Zmodem、TFTP クライアント
SSH（クライアント、サーバー）、Telnet（サーバー、クライアント）、
SNMP エージェント（SMNPv1）、トラップ

a. AT-FL-08（別売）が必要
b. AT-FL-04（別売）が必要
c. AT-FL-05（別売）が必要
d. AT-FL-06（別売）が必要
e. AT-FL-15（別売）が必要
f. サービスが対応していれば同時 5 セッション可

B.1 保証について

本製品の保証内容は、製品に添付されている「製品保証書」の「製品保証規定」に記載されています。製品をご利用になる前にご確認ください。本製品の故障の際は、保証期間の内外にかかわらず、弊社修理受付窓口へご連絡ください。

アライドテレシス株式会社 修理受付窓口

Tel: 0120-860332
携帯電話／PHS からは : 045-476-6218
月～金（祝・祭日を除く）9:00 ～ 12:00、13:00 ～ 17:00

保証の制限

本製品の使用または使用不能によって生じたいかなる損害（人の生命・身体に対する被害、事業の中断、事業情報の損失またはその他の金銭的損害を含み、またこれらに限定されない）につきましては、弊社はその責をいっさい負わないこととします。

B.2 ユーザーサポート

障害回避などのユーザーサポートは、次の「サポートに必要な情報」をご確認のうえ、弊社サポートセンターへご連絡ください。

アライドテレシス株式会社 サポートセンター

http://www.allied-telesis.co.jp/support/info/
Tel: 0120-860772
携帯電話／PHS からは : 045-476-6203
月～金（祝・祭日を除く）9:00 ～ 12:00、13:00 ～ 18:00

サポートに必要な情報

お客様の環境で発生した様々な障害の原因を突き止め、迅速な障害の解消を行うために、弊社担当者が障害の発生した環境を理解できるよう、以下の点についてお知らせください。なお、都合により連絡が遅れることもございますが、あらかじめご了承ください。

1 一般事項

すでに「サポート ID 番号」を取得している場合、サポート ID 番号をお知らせください。サポート ID 番号をご記入いただいた場合には、ご連絡先などの詳細は省略していただいてかまいません。

- サポートの依頼日
- お客様の会社名、ご担当者名
- ご連絡先
- ご購入先

2 製品について

製品名、製品のシリアル番号（S/N）、製品リビジョンコード（Rev）などのハードウェア情報をお知らせください。
これらの情報は、本体底面に貼付されているシリアル番号シールに記入されています。

（例）
S/N 000770000002346 Rev 1A

PIC（AR020、AR021 V2）をご使用の場合は、PIC 名、PIC のシリアル番号（S/N）とリビジョンコード（Rev）もお知らせください。これらの情報は、PIC の基板に貼付されているシリアル番号シールに記入されています。

ファームウェアの「Software Version」をご記入ください。これらは、Manager または Security Officer レベルでログインし、「SHOW SYSTEM」コマンドで確認できます。図 B.2.1 に例を示します（日付などは一例です）。

```
 login: manager
Password: xxxxxxx（お客様の環境におけるものを入力）

Manager >SHOW SYSTEM ↵

Router System Status                              Time 01:36:14 Date 05-Apr-2006.
Board       ID Bay  Board Name              Host Id Rev    Serial number
-----------------------------------------------------------------------------
Base       257     AR570S                          0 M2-0   D1656101A
PIC         75   0  AT-AR020-00 PIC E1/T1 PRI      0 M2-0   50087737
-----------------------------------------------------------------------------
Memory -   DRAM :131072 kB    FLASH : 32768 kB
Chip Revisions -
-----------------------------------------------------------------------------
SysDescription
CentreCOM AR570S version 2.7.5.B-03 09-Mar-2006
SysContact

SysLocation

SysName
OSAKA
SysDistName

SysUpTime
68586 ( 00:11:25 )
Boot Image       : 570-104.fbr size 771920 2[illegible]-Mar-2006
Software Version: 2.7.5.B-03 09-Mar-2006
Release Version : 2.7.5.B-00 20-Oct-2005
 .....
```

図 B.2.1 サポートに必要なソフトウェア情報

3 お問い合わせ内容について

どのような症状が発生するのか、またそれはどのような状況で発生するのかをできる限り具体的に（再現できるように）お知らせください。

可能であれば、早期解決のために、エラーメッセージやエラーコード、設定スクリプトファイルをお送りください（パスワードや固有名など差し障りのある情報は、抹消してお送りくださいますようお願いいたします）。

4 ネットワーク構成について

ネットワークとの接続状況や、使用されているネットワーク機器がわかる簡単な図をあわせてお送りください。

他社の製品をご使用の場合は、メーカー名、機種名、バージョンなどをお知らせください。

☆☆☆

ご注意

本書に関する著作権などの知的財産権は、アライドテレシス株式会社（弊社）の親会社であるアライドテレシスホールディングス株式会社が所有しています。アライドテレシスホールディングス株式会社の同意を得ることなく本書の全体または一部をコピーまたは転載しないでください。
弊社は、予告なく本書の一部または全体を修正、変更することがあります。
弊社は、改良のため製品の仕様を予告なく変更することがあります。

商標について

CentreCOM は、アライドテレシスホールディングス株式会社の登録商標です。
Windows および Windows NT は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
その他、この文書に掲載しているソフトウェアおよび周辺機器の名称は各メーカーの商標または登録商標です。

電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

廃棄方法について

本製品を廃棄する場合は、法令・条例などに従って処理してください。詳しくは、各地方自治体へお問い合わせいただきますようお願いいたします。

日本国外での使用について

弊社製品を日本国外へ持ち出されるお客様は、下記窓口へご相談ください。

Tel: 0120-860442
月～金（祝・祭日を除く）9:00 ～ 17:30

マニュアルバージョン

2006 年 4 月　Rev.A　初版（Firmware Ver.2.7.5.B-03）